Herbjørn Andresen

Tilgang til og videreformidling av helseopplysninger

Regulering og kontroll på tvers av IT-systemer og organisatoriske grenser

Manuskript innlevert til bedømmelse for ph.d.-graden ved
Det juridiske fakultet, Universitetet i Oslo, 15. april 2010

Innhold

1 Innledning

1.1 Emne og omfang

Denne avhandlingen er en tverrfaglig behandling av emnet *tilgang til og videreformidling av helseopplysninger*. Uten å etablere en formell definisjon kan man si at tilgang er å ha eller å kunne skaffe seg kjennskap til en pasients helseopplysninger. Videreformidling er å bidra til at andre får tilgang.[1] Tilganger er begrenset av et konfidensialitetsvern, som tilsier at ingen skal ha tilgang uten legitimt behov for det. Taushetsplikten gir et grunnleggende vern mot uberettiget videreformidling.

Den faglige forankringen er forvaltningsinformatikk. Ved Universitetet i Oslo er Avdeling for forvaltningsinformatikk etablert som et tverrfaglig forskningsmiljø, knyttet til Senter for rettsinformatikk ved Det juridiske fakultet. Forvaltningsinformatikken forener juridiske, informatiske og samfunnsfaglige perspektiver på ulike problemstillinger som er relevante for bruk av informasjonsteknologi i offentlig forvaltning og i andre forvaltningslignende institusjoner i samfunnet.

Avhandlingen inngår i prosjektet *iAccess – Integrated Access Control for Health Care Information Systems*, som er et samarbeid mellom Avdeling for forvaltningsinformatikk, NTNU og SINTEF. Prosjektet er finansiert av Norges Forskningsråd, under programmet IKT Sikkerhet og sårbarhet. Denne avhandlingens emne omfatter sentrale deler av prosjektets uttalte hovedmål:

> Hovedmålet for iAccess er å studere prinsipper og utvikle en modell for integrert tilgangskontroll i helseinformasjonssystemer. Ved å gjøre dette ønsker prosjektet å

[1] Ordet videreformidling er valgt her fordi det er brukt i samme betydning i EUs personverndirektiv, EP/Rdir 95/46/EF. Det vil omfatte både overføring av opplysninger til en annen og det å tildele noen en tilgangsmulighet uten at opplysninger overføres. Ren transport av opplysninger, der transportøren ikke blir kjent med opplysningenes innhold, er imidlertid ikke omfattet av begrepet videreformidling slik det brukes her.

> bidra innen forskning på tilgangskontroll og legge til rette for mer effektiv og sikker informasjonsspredning i det fremtidige helsevesenet.[2]

Helseopplysninger er legaldefinert i helseregisterloven.[3] Definisjonen er vid nok til å omfatte det meste av opplysninger som kan knyttes til en person, i egenskap av at vedkommende er eller har vært pasient. Grensedragninger rundt definisjonen er det liten grunn til å problematisere her. Det er mange trekk ved helseopplysningene som bidrar til at dette blir et mer omfattende emne. Helseopplysningene oppstår bokstavelig talt i pasientens kropp, berettes om i konsultasjoner, fortolkes i dokumentasjonsprosesser, tallfestes i laboratorier og måleapparater, detaljeres og suppleres i den medisinske behandlingen. Videre brukes de med eller uten pasientens innflytelse til administrasjon og kontroll av refusjonsoppgjør, som kriterier for velferdsytelser, i noen tilfeller som ledd i dokumentasjonen som ligger til grunn for myndighetsinngrep, som data i medisinsk og helsefaglig forskning, eller som grunnlag for å nekte forsikring. Helseopplysninger omdannes i en del tilfeller fra vurderinger til kodete verdier, og brukes som grunnlag i nye vurderinger. De akkumuleres over lang tid, og hos mange ulike aktører. Det er ofte betryggende, og til pasientens fordel, men det kan også bidra til et ubehag eller en konkret ulempe for pasienten. Prinsipielt sett er hele bredden av de sammenhengene en helseopplysning kan inngå i over tid og mellom aktører innbefattet i avhandlingens emne. Det konkrete omfanget er imidlertid begrenset til relativt få eksempler på systemer, miljøer og formål som kan illustrere denne bredden.

Selv om rettsreglenes grunnposisjon er at tilgang og videreformidling er underlagt restriksjoner, dreier det seg likevel ikke om sjeldne og ekstraordinære foreteelser. Produksjon, bruk, omdanning og gjenbruk av helseopplysninger, i samspill mellom flere aktører, inngår i en lang rekke helt ordinære prosesser. Konfidensialitetsvernet og taushetsplikten inngår som to av flere elementer i reguleringen av og kontrollen med disse prosessene. Omfanget i denne avhandlingen er behandling av helseopplysninger gjennom regulære og presumptivt berettigede prosesser, og håndtering av eventuelle feil og overtredelser i forbindelse med slike prosesser. Sjeldne ad hoc-situasjoner eller særskilt kompliserte grenseoppganger mellom hva som er berettiget og uberettiget vies ikke spesiell oppmerksomhet.

Avhandlingens undertittel er *regulering og kontroll på tvers av IT-systemer og organisatoriske grenser*. At IT-systemer og organisatoriske grenser er angitt som en del av emnet,

---

[2] SINTEF, «iAccess informasjonsside»: *http://www.sintef.no/Informasjons--og-kommunikasjonsteknologi-IKT/Systemutvikling-og-sikkerhet/Prosjekter/iAccess/*.

[3] «[I denne loven forstås med:] helseopplysninger: taushetsbelagte opplysninger i henhold til helsepersonelloven § 21 og andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold, som kan knyttes til en enkeltperson.» Helseregisterloven, 18. mai 2001 nr. 24 § 2(1)(1).

henger sammen med at det dreier seg om behandling av helseopplysninger i regulære prosesser. Det foregår i miljøer, med fysisk og teknologisk infrastruktur, med kjente aktører og ansvarsforhold. Uttrykket «på tvers av» viser imidlertid til en utvikling som foreløpig er i en relativt tidlig fase. Prosessene for behandling av helseopplysninger beveger seg i økende grad i retning av horisontal integrasjon på tvers av teknologiske og organisatoriske miljøer.

Regulering gjelder spørsmålet om hva som er berettiget tilgang og videreformidling, mens kontrollspørsmålet handler om hvordan dette kan sikres og godtgjøres. Man kommer imidlertid ikke langt med bare de to spørreordene hva og hvordan. Emnet kan detaljeres ved å innføre flere spørreord, blant annet hvem skal ha tilgang, tilgang til hva og om hvem, hvorfor er det behov for tilgang, og når er det behov for den? Videre kan man spørre om berettigelsen skal være avhengig av pasientens aksept eller ikke. Listen over spørsmål kan gjøres lengre, men foreløpig er den primært ment som en illustrasjon. Kontrollmetodene vil måtte ta opp i seg de samme spørsmålene: Hvem får tilgang, hva får vedkommende tilgang til, hvilke kriterier berettiger tilgangen, når gjelder den? Den eventuelle medbestemmelsen, som pasienten har hatt adgang til å utøve, må også kunne kontrolleres.

Ordet regulering innebærer her at utgangspunktet for å vurdere berettigelse er rettslige normer, underlagt rettssystemets metoder, konvensjoner og institusjoner. Likevel oppfattes det konkrete og operative arbeidet med å ta stilling til hva som gir berettigelse, med tilhørende håndheving og etterprøving, i større grad som hjemmehørende i fagdisipliner som informasjonssikkerhet og helseinformatikk. I disse fagene utgjør det som konvensjonelt sett regnes som rettssystemet bare en begrenset del av grunnlaget for arbeidet. Reguleringen kan ses som et flettverk av konkrete rettsregler og mer indirekte regulering gjennom plikter til å utøve selvregulering, ta hensyn til faglige normer, og innordne seg politiske og økonomiske premisser. Samfunnets kontroll med reguleringen blir i stor grad ivaretatt av statlige tilsynsorganer, i denne sammenhengen Helsetilsynet og Datatilsynet, med et sammensatt rettslig og faglig-politisk mandat. Dette innebærer ikke på noen måte at reguleringen forlater den rettslige sfære, den utvikles i et hybrid felt som både er rettslig, teknologidrevet og faglig-politisk.[4]

Tilgangskontroll er en godt innarbeidet fellesbetegnelse for metoder, teknologiske prinsipper og verktøy for å kontrollere tilgang til opplysninger. Avhengig av hvor sofistikert modellen for tilgangskontroll er, vil betegnelsen også omfatte kontroll med flere typer hand-

[4] Dette kan også analyseres som et utviklingstrekk med til dels betydelige konsekvenser for hva retten er og kan være, se for eksempel Inger-Johanne Sand (2005): «Retten i det polykontekstuelle samfunn. Hvordan skal vi analysere og forstå den?». I: *Retfærd. Nordisk Juridisk Tidsskrift,* s. 1–28. (særlig s. 6–8).

linger enn å skaffe seg tilgang. Kontroll med videreformidling av opplysninger inngår i en del modeller for tilgangskontroll, men ikke i alle. Det er primært *autorisasjonskontroll*, som er den delen av tilgangskontrollen som uttrykker tillatelser og forbud, som er gjenstand for undersøkelser og drøfting. Andre sider ved tilgangskontroll, for eksempel det å sikre at en person er den han gir seg ut for å være, ligger utenfor avhandlingens omfang.

Som grovmasket hovedinndeling har reguleringssiden en juridisk kjerne, mens kontrollsiden har en teknologisk kjerne. Det ville likevel være en for stor forenkling å dele avhandlingen inn i avgrensede faglige bolker etter dette skillet. Kontrollaktivitetene er mer enn teknologi, de er også omgitt av plikter og rettigheter. Samtidig er den aktørrelasjonen som er tydeligst til stede i rettskildene på området, relasjonen mellom helsepersonell og pasient, mindre problematisk enn både relasjonen mellom to virksomheter og relasjonen mellom virksomhet og ansatt. Derfor er også reguleringssiden tjent med å bringe inn andre faglige perspektiver og kilder enn det som vanligvis kalles rettskilder. Kanskje er det mer treffende å se regulering og kontroll som to sider av samme sak enn som motpoler.

1.2 Problemstilling

Avhandlingens innerste og mest konsise problemstilling er om, og i så fall hvordan, det er mulig å oppnå samsvar mellom reglene om og kontrollen med berettiget tilgang til og videreformidling av helseopplysninger. Et utgangspunkt for denne problemstillingen er følgende setning i helseregisterloven:

> Tilgang kan bare gis i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt.[5]

Betingelsen er, tilforlatelig nok, at det må være samsvar mellom legitimerende grunner og praksis. Det grunnleggende spørsmålet, hvorvidt og hvordan dette er mulig, kan omformes til følgende forskningsspørsmål:

> *Hva slags teknologiske representasjoner av regler om tilgang til og videreformidling av helseopplysninger er best egnet til å innfri kravet til samsvar?*

Den mest direkte strategien for å besvare dette spørsmålet er å gjennomgå ulike teknologiske prinsipper for kontroll, og vurdere hvor godt egnet de er til å representere de to kriteriene

[5] Helseregisterloven § 13(1) annet punktum.

«nødvendig for vedkommendes arbeid» og «i samsvar med gjeldende bestemmelser om taushetsplikt». En slik undersøkelse gjennomføres i avhandlingens siste del.

Imidlertid er verken tolkning av de legitimerende kriteriene, eller ekstrahering av det som kan være relevante teknologiske prinsipper, opplagt eller selvforklarende. Store deler av avhandlingen vies til å bygge opp og begrunne noen forutsetninger for å vurdere hvor godt noen ulike kontrollprinsipper vil være egnet til å sikre dette samsvaret. Disse forutsetningene vil nødvendigvis være tverrfaglige. Arbeidet med å utforme dem tar utgangspunkt i noen heuristiske, eller erfaringsbaserte, spørsmål av sammensatt rettslig, informatisk, normteoretisk, organisasjonsteoretisk og sikkerhetsfaglig art.

Et vesentlig kriterium i vurderingen er hva som er, eller kan være, subsidiære egenskaper dersom samsvaret er for svakt. Dette omfatter både spørsmålet om hvor store avvik som er akseptable, og hvor gode korrigerende tiltak det er mulig å etablere. Et annet moment er samspillet mellom virksomhetsnivået, altså de som beslutter og administrerer tilganger, og hver ansatt som utfører enkeltoppgaver innenfor rammene virksomheten setter. Det er et relativt komplekst felt som blant annet omfatter spørsmål om hva som er ulike aktørers oppgaver, ansvar og handlingsrom. Videre reiser bruk av helseopplysninger til forskjellige formål, og på tvers av virksomhetsgrenser og teknologiske miljøer, spørsmål om hvordan og hvor godt det er mulig å harmonisere kontrollen med tilgang og videreformidling under skiftende omstendigheter. Et mer subtilt spørsmål i den forbindelse er om et harmonisert sikkerhetsnivå horisontalt mellom virksomheter er nødvendig, eller hensiktsmessig, for å oppnå legitimerende grunner for tilgang og praksis. Sist, men ikke minst, kommer spørsmålene om hvilken betydning pasientens rettigheter, interesser og muligheter for å påvirke behandlingen av opplysninger har for kriteriene som berettiger tilgang og videreformidling.

Spørsmålene ovenfor gir et grunnlag for å utforme de forutsetningene som oppstilles for en egnethetsvurdering. De er imidlertid ikke utformet som distinkte forskningsspørsmål som besvares hver for seg. Spørsmålene er eltet sammen og omdisponert til en mer deskriptiv fremstilling av de enkelte forutsetningene. Noen av forutsetningene drøftes relativt kortfattet, og kvitteres ut ved å referere til annen teori. Det er imidlertid også en del av forutsetningene som er basert på egne analyser og undersøkelser, med ulike typer metodisk belegg. Forutsetningene som utvikles i avhandlingen er påstander om verden, som hver for seg kan aksepteres eller bestrides. Disse påstandene er like viktige bidrag til å forstå avhandlingens emne som den konkrete egnethetsvurderingen som følger av den initielle hovedproblemstillingen.

1.3 Faglig og metodisk opplegg

Målet for forvaltningsinformatisk forskning er en type tverrfaglig sammenhengskunnskap. I tråd med dette målet sikter avhandlingen i større grad mot forståelse av prinsipielle trekk ved regulering og kontroll, enn å undersøke nyanser på detaljnivået. Sammenhengene som det metodiske opplegget er innrettet for å undersøke befinner seg på et plan som kanskje kan beskrives som «forholdsvis nær bakkeplanet, men ikke helt nedpå». De tverrfaglige møtene går mellom rettslig prinsipper og systematikker, teknologisk designprinsipper, og teori om organisering. Avhandlingens nivå er altså *ikke* «bakkeplanet», i form av utsagn om gjeldende rett, forslag til design og implementering av IT-systemer, eller analyse av organisasjoners faktiske beslutninger og handlinger. Likevel er det i mange tilfeller nødvendig å bruke eksempler og belegg fra ulike kilder av forholdsvis detaljert og fagspesifikk art, for at undersøkelsene i det hele tatt skal kunne bli anvendelige og virkelighetsnære.

Forvaltningsinformatiske forskningstemaer kan presenteres på ulike vis, for eksempel kan man tenke seg en matrise med to dimensjoner. I den ene dimensjonen kan man plassere ulike emner eller fenomener i samfunnet. Behandling av helseopplysninger på tvers av IT-systemer og organisatoriske grenser er et av svært mange relevante emner som kan stilles opp i en søyle i denne dimensjonen. I matrisens andre dimensjon kan man plassere fagets ulike forskningsfelt, som er en gruppering av beslektede faglige spørsmål. Antallet forskningsfelt er ikke på langt nær så høyt som antallet mulige emner. Det faglige forskningsfeltet som er mest fremtredende i denne avhandlingen, er representasjon av rettslige normer i IT-systemer. To andre forvaltningsinformatiske forskningsfelt som berøres, er informasjonssikkerhet og teknologi som støtter eller styrker personopplysningsvernet.

Behandling av helseopplysninger er et emne som det alltid har vært en viss interesse for i rettsinformatisk og forvaltningsinformatisk forskning, men uten at det i seg selv er et særskilt sentralt eller definerende emne for dette fagmiljøet. Det er et av mange studieobjekter man kan velge seg, og forske på med et «utenfra-blikk». Problemstillinger, metoder og resultater vil både være beriket av og begrenset av forvaltningsinformatikkens faglige fotavtrykk. Kanskje kan det være grunn til en viss uro over hva det faglige fotavtrykket egentlig består i, når man forsøker å trekke sammenhenger mellom så forskjellige autonome disipliner. En slik bekymring kan reformuleres til et spørsmål om hva som gjør dette til en forvaltningsinformatisk avhandling. Svaret ligger neppe i de konkrete metodevalgene, og heller ikke i valget av studieobjekt. Det handler i større grad om den tverrfaglige ambisjonen, graden av slektskap med annen forskning innen faget, og en litt vanskelig begrunnbar fornemmelse av at

i hvert fall noen av resultatene – enten man er enig i dem eller ikke – kanskje ikke hadde vært tilgjengelige uten nettopp denne faglige forankringen.

Et problem ved den tverrfaglige tilnærmingen, som forhåpentligvis vil være et relativt beskjedent problem, er at fremstillingen ikke hører naturlig hjemme i en forutbestemt sjanger. Både vitenskapelige tekster innen et fag, rettskilder og politiske dokumenter tilhører sakprosa-sjangre der forkunnskaper og innlærte forventninger er en integrert del av det å forstå teksten. Disse forventningene kan dreie seg om oppbygging, stil, hvem man henvender seg til, hva man ser behov for å definere nærmere, underforståtte premisser og lignende. Tekstens tilhørighet i en sjanger kan både by på hensiktsmessige snarveier og begrensende tolkningsrammer for den som bruker teksten. Mens metoden gjør forskningen holdbar, kan man kanskje si at sjangeren gjør fremstillingen gangbar.

Et sjangertrekk ved denne avhandlingen, som skiller den fra en del annen forskning, er at det er vanskelig å forutsette noe om leseren. Det som står her bør være forståelig og gangbart for lesere med en hvilken som helst av de fagdisiplinene som er berørt som bakgrunn. Ikke minst må det være forståelig for forfatteren selv. Derfor er antakelig en del momenter på samme tid både grunnere og mer omstendelig drøftet enn det som er vanlig i fagdisiplinene. Detaljrikdom er altså ikke ensbetydende med dybde og kompleksitet, det kan også være et utslag av mangel på hensiktsmessige snarveier. Et annet lite problem, som også kan bidra til omstendelighet i fremstillingen, er at ulike fagdisipliner av og til legger forskjellige meninger i samme ord. Et eksempel er ordet behandling, som både brukes om å gjøre syke mennesker friskere, om innsamling og bruk av opplysninger, og om tekniske operasjoner. Hovedstrategien er å unngå å problematisere overlappende begrepsbruk mer enn høyst nødvendig, men det er neppe forsvarlig å ignorere faren for parallell bruk av begreper fullstendig.

1.3.1 Analysestrategi

Den tverrfaglige problemstillingen innebærer et behov for å belyse emnet fra forskjellige hold, og etter litt ulike opplegg. Dermed får avhandlingen innslag av flere ulike undersøkelses- og analysemetoder. Valg av metoder blir et spørsmål om rett verktøy til det enkelte spørsmål; det er nødvendigvis en viss sammenheng mellom hva man vil kunne finne ut, og måten man prøver å finne det ut på. En kort oversikt over metodiske opplegg, i betydningen planmessige fremgangsmåter i arbeidet, er plassert her i metodekapitlet. Mer detaljerte diskusjoner om metodespørsmål er lagt til de enkelte kapitlene, i den utstrekning det er behov for å begrunne valgene nærmere.

Bruk av ulike metodiske opplegg i forskjellige kapitler medfører en fare for at teksten ikke oppleves som sjangermessig enhetlig. Den overordnede disposisjonen er ment å skulle bøte noe på det: Kapitlene i del I og II utgjør en forutsetning for å besvare hovedproblemstillingen, og i hvert kapittel er det fremsatt mer eller mindre eksplisitte påstander. Hver undersøkelse, analyse eller drøfting dreier seg om å utvinne forutsetningene, og gi belegg for påstandene.

Det metodiske opplegget er altså en forsøksvis enhetlig argumentasjonsstruktur på overordnet nivå. Avhandlingen følger en analytisk bevegelse,[6] der tidligere kapitler brukes som forutsetning for senere analyser. Selv om disposisjonen er ordnet fra det generelle til det mer spesifikke, er det lagt vekt på at analysene skal holde et noenlunde felles abstraksjonsnivå gjennom hele avhandlingen. Analyser og drøftinger er gjennomgående forholdsvis konkrete, også i de kapitlene som drøfter generelle påstander. Belegg, eksempler og bruk av teori er lagt relativt nær det empirisk etterprøvbare, men likevel med større vekt på forklaringsverdi enn på detaljfunn.[7]

Avhandlingens to første deler, som er forutsetninger for analyse av hovedproblemstillingen, er overveiende deskriptive og ikke normative. Hensikten er å si noe om verden, ikke å stille krav til verden. Det innebærer ikke at de deskriptive elementene nødvendigvis er opplagte eller ukontroversielle. De omfatter både påstander med et teoretisk anslag, og eget eller lånt belegg for påstandene. I avhandlingens tredje del finnes det, i en viss begrenset utstrekning, også et normativt anliggende. Det skal vurderes hvor egnet ulike teknologiske prinsipper vil være for å ivareta samsvar mellom berettigelse av og kontroll med helseopplysninger. Et stykke på vei kan man forestille seg en slik egnethetsvurdering som en nøytral anvendelse av noen vurderingskriterier mot et forelegg av fortolket regelverk. En nøytral vurdering er imidlertid neppe fullt ut mulig, det er grunn til å anta at samspillet mellom regulering og teknologi også har en refleksiv side. Valg av teknologiske prinsipper kan virke tilbake både på tolkningen og på den fremtidige danningen av regulering. Derfor er det rimelig at egnethetsvurderingen også har rom for utsagn om hvordan samsvaret bør være. Litt uhøytidelig kan den siden ved vurderingen kalles en drøfting *de techne ferenda*.

[6] Uttrykket er lånt fra Morten Knudsen, *En guide til litteratur om metode, analysestrategi og videnskabsteori* (2009), s. 15: «I bestræbelserne på at være så bevidst som muligt om hvad man gør i sine analyser, kan det være nyttigt at overveje, hvilken analytisk bevægelse man foretager. … Man kan se på sit projekt som noget der består af elementer, der gør noget ved hinanden. Det kan fx være, at nogle dele af projektet skal *forklare* andre dele.»

[7] Nivået er sammenlignbart med sosiologen Robert Mertons velkjente begrep *middle range theory*, som kan forstås slik at det legges større vekt på å holde fast ved sammenhengen mellom teori og empiri, enn at en teori kan tilby allmenngyldighet eller lovmessighet.

1.3.2 Kriterier for vederheftighet

Å utvinne forutsetningene er en metafor, med assosiasjoner både til det å hente ut råvarer fra naturen, og til å foredle dem. Nettopp den tvetydigheten bidrar til at det er hensiktsmessig å bruke uttrykket «utvinne» her. Det forener et sammensatt deduktivt og induktivt forløp. Det deduktive dreier seg om å avdekke, finne og analysere forutsetninger, ved at de utledes fra andre forutsetninger eller spørsmål. Samtidig er utvinning av forutsetninger en induktiv aktivitet som går ut på å sette sammen enkeltelementene i materialet slik at de fungerer for formålet. Det er kanskje som slike synteser, eller konstruksjoner, at forutsetningene er mest sårbare for metodiske innvendinger. Når de enkelte elementene i en forutsetning utledes deduktivt, beror hver avgrensning og utelatelse på en vurdering av relevans for formålet. Kriteriene for hvordan en sammensatt forutsetning bygges opp, er derimot mindre entydige. Hvilke elementer av regulering, praksis og kunnskaper om helseopplysninger, systemer og aktører som til slutt anses å høre sammen som en forutsetning for å besvare den initielle problemstillingen, er et resultat av omfattende tolkning og bearbeiding. Andre måter å sette sammen materialet på er mulig, og har også vært prøvd ut underveis. Resultatet skal være holdbart, men kan ikke gjøre krav på å være den eneste fremstillingen av forutsetningene som vil være holdbar.[8]

Det overordnede kriteriet for holdbarhet i denne avhandlingen er det som kan kalles vederheftighet. Vitenskapelig vederheftighet er kanskje i større grad en subjektiv innstilling og erkjent forpliktelse til å overholde vitenskapssamfunnets normer enn et metodisk opplegg. Nedenstående forklaring av kravet til vederheftighet viser imidlertid også til andre kriterier enn forskerens innstilling. Kriteriene er ikke spesielt utfyllende, men de er objektive i den forstand at de kan brukes til å vurdere om resultatet er en vederheftig tekst eller ikke.

> Kravet om «vederheftighet» skal her … innebære følgende: Påstander som ikke bygger på allment etablerte sannheter i vitenskapssamfunnet skal belegges gjennom henvisninger og eksempler, eller begrunnes – dersom de ikke uttrykkelig framstår som frie meningsytringer. Dersom selvmotsigelser forekommer, må de drøftes eksplisitt, for eksempel som paradokser. Dessuten forutsetter alminnelig vederheftighet at taleren/skribenten holder det han lover, blant annet når han redegjør for hva han vil ta opp i sin tekst.[9]

[8] Holdbarhet som kriterium er fra begrepsparet holdbar/uholdbar i Svein Eng (2007): *Rettsfilosofi*. Dette begrepsparet er mer treffende enn for eksempel riktig/galt eller sant/usant, særlig der flere alternative svar kan tenkes å være holdbare eller uholdbare. I likhet med mer tradisjonelle vitenskapelighetskriterier som reliabilitet og validitet er også holdbarhet en form for tilstrekkelighetsnorm.
[9] Johan L. Tønnesson (2001): *Vitenskapens stemmer*, s. 201.

I enkelte deler av avhandlingen er det gjennomført egne undersøkelser og drøftinger i dybden, som har krevd et mer detaljert metodisk opplegg. Kravet til vederheftighet innebærer at også kriteriene for vitenskapelighet, innen de metoder som til en hver tid brukes, skal være oppfylt.

1.3.3 Kildebruk og kildekritikk

Store deler av materialet som analyseres i avhandlingen, er tekstkilder av ulike slag. En del av kildene er vitenskapelige tekster fra de enkelte fagdisiplinene. En annen omfattende gruppe er lover, forskrifter og rettsavgjørelser med videre, som gjerne omtales som rettskilder. Dersom man skulle anvende en renskåren juridisk metode, for å løse et rettslig spørsmål, ville den synsvinkelen man betraktet kildene fra handle om relevans og vekt som rettskilder. For eksempel kunne en offentlig utredning tillegges vekt som argumentkilde for et rettslig resonnement i egenskap av å være forarbeid til en lov. Den samme offentlige utredningen kan imidlertid også være kilde til kunnskaper, argumenter og posisjoner som ikke er av juridisk art. Det er altså ikke nødvendigvis en entydig sammenheng mellom typen dokument og hvilken kildemessig funksjon dokumentet har. Noen av kildene som brukes her passer verken inn i kategorien vitenskapelige tekster eller i det man vanligvis oppfatter som rettskilder.

Kildematerialet brukes på begge sider av det sammensatte deduktive og induktive forløpet. De forutsetningene som utvinnes er ofte en syntese av elementer som enten er inspirert av, eller hentet direkte fra, ulike kilder. Kildene brukes da til å konstruere en sammenheng. I det deduktive forløpet brukes kildene primært til å etterprøve påstander og argumenter. En kildehenvisning kan altså opptre i to prinsipielt ulike funksjoner, både som ledd i å konstruere en sammenheng og som etterprøving. De to funksjonene er ytterpunkter, den enkelte kildehenvisnings funksjon er oftest vanskelig å plassere helt entydig i praksis. Hensikten med å stille opp de to ytterpunktene er å synliggjøre bredden i hva kildene brukes til.

Vederheftig kildebruk er et metodeanliggende. Med det store tilfanget av kilder som kan være aktuelle i et tverrfaglig arbeid som dette, blir vurdering av kildene kanskje enda viktigere enn i fagdisipliner med en mer enhetlig metodetradisjon. Begrepet kildekritikk stammer fra historiefaget, og brukes om forskningsmetoder for å etterprøve en rekonstruksjon fra fragmentene av historien. I utgangspunktet er dette omtrent de samme to funksjonene som er nevnt ovenfor, etterprøving og (re)konstruksjon. Det er likevel store forskjeller mellom historikerens behov for å granske sitt kildemateriale og bruken av kilder som belegg i denne avhandlingen. En innføringsbok i historiefaget beskriver kildekritikk som «et sett av håndverksregler som sier hvordan en skal behandle kilder for ikke å forvri den informasjon en

får ut av dem.»[10] Ved siden av å vektlegge et praktisk perspektiv, er dette også en forsiktighetsnorm. Vederheftig kildebruk fordrer bevissthet om hva en kilde kan gi belegg for, og om hvor solid dette belegget er.

Kildekritikk har en viss utbredelse utenfor historiefaget, for eksempel i nyhetsmediene. Det kunne imidlertid med fordel hatt større oppmerksomhet i andre vitenskapsdisipliner enn historieforskning, ettersom kildehenvisninger av ulike slag er utbredt i de fleste fag. I den første doktoravhandlingen fra Avdeling for forvaltningsinformatikk, som analyserte trekk ved Schengen informasjonssystem (SIS), var metoderedegjørelsen primært viet betraktninger om kildekritikk. Sentrale deler av kildematerialet var nåtidige og flyktige dokumenter som i mange tilfeller bare var tilgjengeliggjort på Internett. Dermed så kandidaten behov for å drøfte vurderingskriterier spesielt tilpasset kildenes art.[11]

De fleste kildene som er brukt i denne avhandlingen har tydelige avsendere, og har inngått i en robust utgivelsesprosess. Derfor er det mindre behov for vurderingskriterier som gransker den ytre troverdigheten. Vurderingene her dreier seg primært om kriterier for hvilke kilder som velges ut, og om å unngå at belegget strekkes lenger enn det er dekning for.

Den første aktiviteten, i kronologisk forstand, som har å gjøre med utvelgelse av kilder er søking og fremfinning. I noen situasjoner, kanskje særlig når kildebrukens hovedfunksjon er etterprøving, vil en forhåndsdefinert avgrensning av hvor man søker og hva man leter etter kunne styrke resultatets pålitelighet. For eksempel kan en forhåndsdefinert avgrensning bidra til å godtgjøre at et samlet kildekorpus innen et område har vært oppe til vurdering. I andre situasjoner, når bruk av kilder til å utvinne teoretiske posisjoner, påstander og argumenter er minst like viktig som etterprøvingen, vil derimot strenge føringer for søkeaktiviteten kunne begrense mulighetene for å oppdage sammenhenger og justere antakelser underveis. Derfor er ikke kildetilfanget for denne avhandlingen avgrenset på forhånd, kildene som er funnet frem er bare underlagt en etterskuddsvis vurdering etter kriteriene som er satt opp nedenfor. Kostnaden ved denne fremgangsmåten er at kildebruken ikke gir en fullstendig dekning av ett eller flere områder.

Når en kilde først har fanget interesse, og kan tenkes å være brukbar til å belyse eller verifisere noe, blir den gjenstand for vurdering etter et sett med kriterier. Her er kriteriene verken ordnet kronologisk eller etter viktighet. Ett kriterium er om den innsikt eller oppfatning som teksten gir inspirasjon til eller belegg for, er sentral eller perifer i den aktuelle

[10] Knut Kjeldstadli (1999): *Fortida er ikke hva den en gang var*, s. 169.
[11] Stephen Kabera Karanja (2008): *Transparency and proportionality in the Schengen Information System and border control co-operation*, s. 17–20.

kilden. For eksempel er det ofte grunn til forsiktighet i omgang med informatiske artiklers utlegning av helseopplysningers beskyttelsesbehov. Dersom en artikkel demonstrerer en grundig og systematisk analyse av behovet, kan den egne seg som noe man sier seg enig i eller ikke. Beskrivelsen av beskyttelsesbehovet kan da sammenholdes med det som fremgår av andre kilder. I mange tilfeller finner man imidlertid et mer tilfeldig og kanskje ubegrunnet utsagn om helseopplysninger, mens artikkelens egentlige formål er å begrunne et teknologisk prinsipp for tilgangsstyring. I slike tilfeller er den aktuelle artikkelen ikke egnet som belegg, verken som støtte for eller avvisning av noe som gjelder forståelsen av helseopplysningers beskyttelsesbehov. Det trenger imidlertid ikke diskreditere samme artikkel som kilde til forståelse av det teknologiske prinsippet den drøfter.

Det er ikke alltid slik at den første kilden man støter på, og som kanskje åpner et interessant perspektiv, er den samme som man velger å gå videre med og til sist henvise til. Arbeidet med et spørsmål fører ofte til et behov for å nøste videre i oppgitte referanser og andre beslektede kilder. Utvelgelse og vurdering er en iterativ prosess. For å holde antallet kildehenvisninger noenlunde overkommelig er det ofte nødvendig å velge bort en del kilder som formidler omtrent samme innhold. Imidlertid blir det av og til, særlig når det er grunn til å vente at en påstand kan virke litt fremmedartet eller kontroversiell, behov for å vise til et mer solid belegg. Da kan flere kilder som formidler det samme, fortrinnsvis kilder som er uavhengige av hverandre eller har ulike funksjoner, være tatt med.

Den tverrfaglige fremstillingen synliggjør at ulike fagtradisjoner kan legge sine føringer for hvilken kilde som skal få representere en bestemt innsikt eller oppfatning. I informatisk litteratur er det ofte en uskreven faglig kanon som ligger til grunn for henvisningspraksis. En analyse av et grunnleggende spørsmål innen en bestemt spesialisering står i fare for å virke lite tillitvekkende dersom referanser til pionerarbeider innen samme grunnleggende spørsmål mangler. Ofte vil det også være referanser til sentrale arbeider som er forgreninger fra pionerarbeidet, og som leder opp mot den aktuelle analysen. Behovet for å kjenne historien synes å være mer enn jåleri, det plasserer teksten innenfor fagfellesskapet og styrker de felles referanserammene. Føringen er at utvelgelsen av en representativ kilde bør ha faghistorisk forankring.

En litt stivere slektning av den uskrevne faglige kanon er bibliometrien. Det finnes noen forskjellige, men ikke universelle, målestokker for å sammenligne vitenskapelige arbeiders innflytelse eller vekt. For eksempel kan antallet henvisninger til en artikkel telles, eller publiseringskanalene kan rangeres etter omdømme ut fra mer eller mindre fastlagte kriterier. Bruk av bibliometri som element i en kildekritikk har imidlertid noen problematiske sider. For

det første er målestokkene forskjellige og lite sammenlignbare. Dernest, så langt størrelsene kan sammenlignes, er det likevel bare et uttrykk for hver av tekstenes egenvekt. Om tekst A scorer høyest, kan likevel tekst B være best egnet som belegg i en konkret kildebruks-sammenheng.[12]

Et annet kriterium, som er nærmest det motsatte av å følge en faghistorisk kanon, er å velge en representativ kilde ut fra en aktualitetsvurdering. I rettsvitenskapen – paradoksalt nok, fordi dette er et gammelt fag, mens informatikken er ung – er det oftere forventet at man utviser stødig kunnskap om den seneste utvikling. Forklaringen er nærliggende, fagets hoved-anliggende er utsagn om gjeldende rett. Etter dette kriteriet er føringen at det som siteres bør være ferskvare. Dette vil imidlertid ikke være rendyrket i alle deler av rettsvitenskapen, i bredere analyser av et fenomen vil det ofte være brukt kilder som dokumenterer en rettsut-vikling.

Andre kriterier for utvelgelse kan også gjøre seg gjeldende. Innen samfunnsfag som sosiologi og statsvitenskap vil det ofte være teoretiske skoler, og slektskap eller motsetninger mellom skoleretningene, som legger føringene. Dessuten, men kanskje ikke like stuerent, er det av og til fristende å velge én kilde fremfor en annen på grunn av en særskilt god formulering. Det innebærer selvfølgelig ikke noe amnesti fra øvrige vurderingskriterier.

En forsiktighetsnorm tilsier at man prøver å vurdere kilden på dens egne premisser. En vitenskapelig tekst inngår som oftest i en kommunikasjon med andre vitenskapelige tekster, gjennom kildehenvisninger og gjengse forutsetninger innen en fagtradisjon. Å bruke kilder fra flere ulike fagtradisjoner krever at man er oppmerksom på faren for å forstrekke teksten, ved å innfortolke noe som kanskje er gjengse forutsetninger i et annet fag enn det kilden hører hjemme i. En annen side ved forsiktighetsnormen er et valg om, i hovedsak, ikke å hente ut mer av en kilde enn det eksplisitt uttrykte meningsinnholdet. Det eksplisitt uttrykte vil av og til kunne ha et snevrere innhold enn det avsenderen «egentlig» sier. Ulike språklige virkemid-ler, og utelatelser, kan bidra til at en leser oppfatter undertekst som ikke ville komme til syne i et direkte sitat. For de fleste formål i denne avhandlingen trekkes ikke mer ut av en kilde enn det den uttrykker eksplisitt. I noen sjeldne tilfeller er det imidlertid likevel nødvendig å fravike dette prinsippet, og da blir det redegjort for hva som innfortolkes. Tendenskritikk, for eksempel for å avdekke sammenhenger mellom avsenders interesser og virkelighetsbeskri-

[12] Kvantitative mål for en rettskildes innflytelse fører til samme type problem. For eksempel er Lovdatas «popularitetsvekt» et toleddet uttrykk for hvor mange dokumenter som henviser til kilden, og i hvor mange ulike kildetyper, altså ulike databaser i Lovdatas system, slike henvisninger finnes. Sykejournaldommen, Rt. 1977 s. 1035, har en svært høy score (P-vekt 72:11, lesedato 14. april 2010). Det skyldes imidlertid primært dens generelle betydning i rettskildelæren, og bare i mindre grad dens konkrete betydning for pasienters innsynsrett, som er grunnen til at kilden er referert i denne avhandlingen.

velse, er av og til nødvendig under drøfting av de forslag til regulering eller kontrolltiltak som noen har fremsatt. Det er imidlertid ikke et mål i seg selv å analysere kildenes språklige virkemiddelbruk, hovedsaken er å sikre at de utvalgte kildene er tilstrekkelig egnede og pålitelige som belegg for det de brukes til her.

Disse momentene om kritisk utvalg og bruk av kilder er en slags dekomposisjon, for å vise hvilken type vurderinger som gjøres. Det er også redegjort for noen forutsetninger, både for hvilke muligheter og hvilke begrensninger vurderingskriteriene gir for hva som kan trekkes ut av kildematerialet. Kriteriene er imidlertid ikke brukt som en systematisk sjekkliste, det konkrete arbeidet med kildene er basert på sammensatte og til dels intuitive vurderinger.

1.3.4 Metodevalg for enkeltundersøkelser

Mens kildekritikk er et metodeperspektiv som er gjennomgående nødvendig i alle deler av avhandlingen, er de enkelte analysene og undersøkelsene i ulike kapitler basert på litt ulike metoder, avhengig av hva som er hensiktsmessig og gjennomførbart.

Utvinningen av teoretiske forutsetninger er i stor grad basert på analyser der elementer fra reguleringen, kontrolltiltakene eller trekk ved behandlingen av helseopplysninger som sådan drøftes i lys av teoretiske perspektiver. Valg av fagperspektiv gir seg ofte selv, for eksempel er et samfunnsvitenskapelig perspektiv naturlig når temaet er klassifisering av aktører.

Også de to kapitlene som i størst grad omhandler rettslig regulering, kapittel 4 om internkontroll som reguleringsmetode og kapittel 6 om helseopplysninger som gjenstand for regulering, er systematiske analyser med et bredere perspektiv enn det rettsdogmatiske. Slike bredere analyser er ikke ukjent eller uhørt innenfor den juridiske faglitteraturen. I sin artikkel om hva som kan kjennetegne fremtidige rettsvitenskapelige avhandlinger, deler Sandgren inn i fire forskjellige kategorier av arbeider. De fire kategoriene er tradisjonell rettsdogmatikk, rettsanalytiske arbeider, rettsteori og avhandlinger som gjør bruk av utenomrettslige teorier og metoder. Som et tverrfaglig arbeid kan denne avhandlingen passe delvis til beskrivelsene av alle de tre siste avhandlingstypene. Ambisjonen om å legge størstedelen av drøftingen nokså nær det empiriske materialet fører imidlertid til at kategorien rettsanalytiske arbeider virker mest treffende for denne avhandlingen.[13]

[13] Forfatteren introduserer kategorien *rättsanalytiska arbeten* slik: « … en mångfald argument och rättskällor används i den rättsvetenskapliga praktiken som alltmer handlar om att analysera rätten snarare än att 'fastställa gällande rätt'.» Claes Sandgren (2007): «Framtidens doktorsavhandlingar i rättsvetenskap». I: *Tidsskrift for Rettsvitenskap,* s. 388–407. (s. 403).

Ett av kapitlene er primært viet de praktiske erfaringene med bruk, regulering og kontroll av helseopplysninger. Datagrunnlaget er til dels eget materiale, samlet inn gjennom en relativt beskjeden skjemaundersøkelse og noen få intervjuer. Funn fra disse undersøkelsene sammenlignes med andre empiriske undersøkelser.

Den mest krevende metodiske utfordringen ligger i å gjennomføre en vurdering av hvor godt egnet ulike kontrollprinsipper vil være for å oppnå best mulig samsvar mellom faktisk kontroll og de grunner som legitimerer tilgang og videreformidling, avhandlingens kapittel 9. Bakgrunn og målestokk for vurderingene er de forutsetningene som er fremstilt og behandlet tidligere i avhandlingen. Et metodisk gyldighetskriterium vil være å yte alle de teknologiske prinsippene som vurderes en viss rettferdighet. Metoden er noe ad hoc-preget og tilpasset dette formålet.

Denne måten å behandle stoffet på har blitt til ved å prøve ut mange spor, holde fast ved noen, og forkaste andre. Ambisjonen er at dette skal være en tilstrekkelig overbevisende måte å behandle stoffet på, det som imidlertid er sikkert er at det ikke er den eneste måten. Det kan derfor være fristende å slutte seg til følgende formulering fra metodekapitlet i Zapffes avhandling fra 1941: «… jeg har fundet det paakrævet i en indledning som denne at gjøre rede for de anfegtelser som meldte sig ved arbeidets begyndelse.» [14]

1.4 Oversikt over fremstillingen

Avhandlingen har tre deler. I del I presenteres, drøftes og undersøkes de forutsetningene som er av mest generell art. De forutsetningene som dreier seg mer konkret om bruk, regulering og håndtering av helseopplysninger, følger i del II. Vurderinger av ulike teknologiske prinsippers egnethet for samsvar med reguleringen er plassert i del III. Fremstillingen følger således en bevegelse fra det generelle til det mer spesifikke. Dermed har ikke avhandlingen skarpt avgrensete rettslige eller teknologiske bolker. Innenfor avhandlingens tre deler veksler de enkelte kapitlene mellom rettslige, teknologiske og samfunnsmessige perspektiver. I noen av kapitlene vil én av fagdisiplinene dominere, mens andre kapitler er mer tverrfaglige.

Dette kapitlet, kapittel 1, forteller hva som er avhandlingens emne og faglige forankring, hvilke fenomener som undersøkes, og hvordan de undersøkes.

Avhandlingens del I, som omfatter kapitlene 2, 3 og 4, er generell bakgrunnsteori på tre ulike områder. Stoffet er generelt i den forstand at det vil kunne være relevant for atskillig

[14] Peter Wessel Zapffe (1996): *Om det tragiske*, s. 14.

flere emner enn det som dekkes av tittelen *tilgang til og videreformidling av helseopplysninger*. Disse kapitlene inneholder selvstendige undersøkelser, begrepsanalyser og belegg for påstander som blir premisser i de to siste delene. I stedet for egne kapitler innledningsvis kunne man tenke seg at bakgrunnsteorien bare ble presentert og drøftet der den brukes. Det ville imidlertid føre til en så tett sammenfletting av generelle og spesifikke emner at både forfatter og leser kunne få problemer med å holde tråden.

Fremstillingsmessig kan kapitlene i første del betegnes som «Tsjekhovs pistoler».[15] I prinsippet er det nærmest ubegrenset hvor mye bakgrunnsteori som kan ha en viss relevans. Det går imidlertid en grei pragmatisk grense for hva slags bakgrunnsteori, og i hvilken dybde og hvilket omfang, som er formålstjenlig i denne avhandlingen. Den viktigste testen på at det som er tatt med av bakgrunnsteori forsvarer sin plass i avhandlingens første del, er at det faktisk brukes senere, og at det er nødvendig i den forstand at kortfattede henvisninger til annen litteratur ikke ville få poengene godt nok frem.

Kapittel 2 presenterer faglige fortolkningsrammer og teoretiske bidrag om teknologistøtte for kontroll med tilganger til og bruk av opplysninger. Disse rammene er delt inn i tre underkapitler, henholdsvis rettsteknologi som rettsinformatisk emne, noen normteoretiske betraktninger, og noen grunnleggende teknologiske prinsipper og begreper innen tilgangskontroll. Kriteriet for at et teoretisk bidrag skal være relevant for denne avhandlingen, er at det har betydning for hvordan teknologiske representasjoner av rettslige regler om berettiget bruk av helseopplysninger kan uttrykkes. Resultatet av kapitlet er et slags bakgrunnsmateriale for utvalg og nærmere vurderinger av prinsipper for kontroll med opplysninger. Hvor godt disse prinsippene er egnet for formålet, og under hvilke betingelser, drøftes mer detaljert i avhandlingens del III.

Kapittel 3 er en klassifisering av aktører, i grupper som har ulike rettslige og praktiske posisjoner. Selve inndelingen i aktørgrupper er for så vidt triviell, men forståelsen av disse posisjonene er grunnleggende for de videre drøftingene. De ulike prinsippene for teknologisk representasjon speiler til dels også forskjellige ideologiske syn på de ulike aktørgruppene. En påstand som utvikles fra dette kapitlet, og som forfølges i større detalj videre, er at den aktørrelasjonen som er mest kompleks og vanskeligst å representere teknologisk, er relasjonen mellom helsetjenestens virksomheter og de enkeltindividene som utfører sitt arbeid som helsepersonell i disse virksomhetene. *Prima facie* ser imidlertid svært mange regler om

[15] En av flere varianter som siteres er: «Hvis en pistol henger på veggen i første akt, må den avfyres i siste akt.» Det er en slags læresetning for dramatikk som stammer fra Anton Tsjekhov; det som skjer på scenen skal begrenses til det som er nødvendig for handlingen. Han skal selv ha uttrykt dette på litt forskjellige vis i samtaler og brev, slik at en presis referanse er vanskelig å oppdrive.

håndtering av helseopplysninger ut som om de fremdeles hovedsakelig dreier seg om forholdet mellom individuelt helsepersonell og en pasient. Hvorvidt helseopplysninger formidles til aktører innenfor eller utenfor helsetjenesten og helseforvaltningen har også viktige rettslige og praktiske følger.

Kapittel 4 er en bredt anlagt analyse av risikobasert internkontroll som reguleringsmetode. Fremstillingen og eksemplene er hentet fra et atskillig bredere materiale enn det som har direkte relevans for kontroll med helseopplysninger. Hensikten er å forsøke å gi dekkende belegg for noen påstander om den rettslige reguleringen av virksomheters arbeid med å sikre visse samfunnsinteresser. Den brede gjennomgangen er nødvendig fordi den inneholder en rekke enkeltelementer som ikke kan leses direkte ut av bare de kildene som omhandler samfunnsområdet helse eller samfunnshensynet informasjonssikkerhet.

Reguleringsmetoden innebærer et relativt stort innslag av selvregulering, og dermed et betydelig handlingsrom for den enkelte virksomhet. Den generelle analysen i kapittel 4 viser at det kan variere en del, både fra rettsområde til rettsområde og fra virksomhetstype til virksomhetstype, hvor frie tøyler en plikt til internkontroll innebærer for virksomheten. Regulering av informasjonssikkerhet og pasientsikkerhet innen helsesektoren ligger imidlertid nær opp til analysens idealtype, med relativt stort handlingsrom for den enkelte virksomhet. En avledet påstand, som følges nærmere opp i del II, er at det gir liten mening å tolke eller praktisere de konkrete reglene om behandling av helseopplysninger, herunder helsepersonells plikter og pasienters rettigheter på området, uten å se dem i sammenheng med virksomhetens plikt til risikobasert styring og operasjonalisering av reglene.

Del II, kapitlene 5, 6 og 7, omhandler helseopplysninger som fenomen. Perspektivet på helseopplysninger beveger seg fra behov og nytteverdi, via rettslig regulering og kontrollregimer, og videre til hvordan de håndteres i praksis.

Kapittel 5 tar for seg hva helseopplysninger er og hvordan de behandles i ulike typer informasjonssystemer. Påstanden i dette kapitlet er at både opplysningenes form, og trekk ved de informasjonssystemene de behandles i, har betydning for regulering av og kontroll med tilgang og videreformidling.

Kapittel 6 går gjennom det rettslige rammeverket for regulering av helseopplysninger. I stedet for en tradisjonell rettsdogmatisk analyse, der et rettsspørsmål besvares gjennom en helhetlig vurdering av kildene, legges det her vekt på å synliggjøre både fellestrekk og innebygde spenninger og motsetninger mellom personopplysningsrettens og helserettens regler om behandling og beskyttelse av helseopplysninger.

Kapittel 7 presenterer empiri om håndtering av helseopplysninger. Empirien er en kombinasjon av egne undersøkelser gjennomført under arbeidet med denne avhandlingen og annen forskning om beslektede spørsmål. Funnene antyder et spenningsforhold, en bred aksept for nytteverdien i økt bruk av helseopplysninger lever side om side med en dyp skepsis til uheldige konsekvenser av dette.

Del III er et nærstudium av kontrollmetoder og kontrollteknologi. Målet er å utforske hvilke metoder og teknologiske prinsipper som i større eller mindre grad er egnet til å ivareta ulike sider ved reguleringen av tilgang til og videreformidling av helseopplysninger.

Kapittel 8 presenterer og begrunner de analytiske vurderingskriteriene som brukes for å bedømme de enkelte metodene og prinsippene som presenteres og drøftes i kapittel 9.

Kapittel 9 er en gjennomgang av flere etablerte og foreslåtte prinsipper for kontroll med berettiget tilgang, bruk eller videreformidling av helseopplysninger. De har varierende praktisk utbredelse og teknologisk modenhet. De første fire prinsippene kan betegnes som konvensjonelle teknologiske prinsipper, alle eksisterer og brukes i ulike sammenhenger både innenfor og utenfor helsesektoren.

De neste seks prinsippene er ulike varianter og suppleringer av konvensjonell tilgangskontroll, som er utviklet eller foreslått som svar på problemer som er spesifikke for helseopplysninger og bruk av IT innen helsesektoren. Disse seks prinsippene er gruppert i tre grupper. To av dem kan kalles aktualiseringsmekanismer, og innebærer en form for ad hoc selvautorisering, innenfor rammer som virksomheten trekker opp. Dernest følger to prinsipper som kan betegnes som forløpsbaserte, det vil si at tilganger tildeles ut fra behov som knyttes til bestemte hendelser eller aktiviteter under behandlingen av en pasient. De to siste av de seks supplerende tilgangsprinsippene går ut på å gi pasienten konkrete muligheter for å styre tilgangene selv.

Etter disse fire pluss seks prinsippene, følger tre prinsipper som kan ses som alternativer til konvensjonell tilgangskontroll. Disse tre siste prinsippene er ikke i utgangspunktet utviklet for å håndtere tilgang til helseopplysninger, de har sitt opphav og sin utbredelse på andre områder. De byr likevel på interessante muligheter, som også kan være relevante for dette formålet.

Det først av de tre siste prinsippene er en nokså uensartet gruppe av teknologier for å spesifisere konkrete regler og betingelser for tilgang til og håndtering av informasjon.[16] Fellestrekket ved denne gruppen er at det utvikles egne språk, med egen konsis syntaks,

[16] En utbredt betegnelse er Policy Expression Languages, eventuelt forkortet PEL. En tentativ oversettelse, som riktignok er noe snevrere, kan være *spesifikasjonsspråk for tilgangspolitikk.*

semantikk og pragmatikk. Dette ligger relativt nær konvensjonell tilgangskontroll, men kan uttrykke mer detaljert og skreddersydd tilgangspolitikk.

Det andre prinsippet i denne gruppen er en parallell til digital rettighetsforvaltning, som er utbredt innen beskyttelse av opphavsrett til åndsverk.[17] Det går ut på å innkapsle regler om bruk i de elektroniske representasjonene av helseopplysningene, og tvinge gjennom håndhevelse i ethvert mottakende system.

Det tredje og siste prinsippet i denne gruppen er bruk av elektroniske agenter, som ivaretar ulike aktørgruppers interesser i systemene. I stedet for å se reguleringer som en mer eller mindre kompleks relasjon mellom betingelse og virkning, er den elektroniske agentens mål å opprettholde en foreskrevet tilstand, uten nødvendigvis å angi i detalj hvordan det skal gå til. Selv om varianter av elektroniske agenter finnes i praksis, og kanskje særlig forbindes med elektronisk handel, er de primært en tankekonstruksjon som ofte beskrives gjennom til dels litt fremmedartede metaforer.

Ingen av de til sammen tretten prinsippene som presenteres og vurderes tilbyr fullstendig treffsikre metoder for kontroll med hele den relevante reguleringen. Valg av teknologisk prinsipp for kontroll innebærer også valg av hvilke deler av reguleringen man velger å betone.

Kapittel 10 avslutter og oppsummerer avhandlingen.

[17] Digital rettighetsforvaltning er en oversettelse av Digital Rights Management. Forkortelsen DRM brukes både for å betegne denne typen kontrollmetode, og som navn på en klasse av elektroniske verktøy til formålet.

Del I:

Generell bakgrunnsteori

2 Teknologistøtte for kontroll med databrukerens handlinger

2.1 Representasjon av rettslige normer i IT-systemer

Et anvendelig begrep for å forklare et IT-system, for eksempel dersom det brukes til å arbeide med pasientjournaler, er at den elektroniske journalen er en representasjon av en god del medisinsk fagkunnskap, administrativ dokumentasjon og noen av de rettslige rammene for journalene. Fra det utsnittet av verden representeres blant annet selve pasienten, som oftest representert ved fødselsnummer og noen få nøkkelopplysninger om vedkommende, medisinske kodeverk for diagnoser og behandlinger, journalføring av hver konsultasjon, vurderinger, henvisninger, med mer.[18] Begrepet representasjon tydeliggjør at IT-systemet er en modell av noe, som gjengir en analysert, fortolket og konstruert – eller designet – versjon av en valgt del av verden.[19]

Et IT-system som inneholder helseopplysninger om enkeltpersoner kommer i berøring med et stort knippe rettslige normer, av ulik karakter. Noen typer rettslige regelverk er bare en del av IT-systemets omgivelser, eller rammebetingelser. Et eksempel kan være regler om offentlige anskaffelser. Slike regelverk vil man ikke kunne finne igjen som representasjoner inni IT-systemet. Det motsatte ytterpunktet er å representere konkrete rettslige betingelser og virkninger som informasjonsmodell og programkode. Disse normene finnes da representert som et rettslig innhold i IT-systemet. Den rendyrkede varianten av dette er mer utbredt i velferdsforvaltningen enn i helsesektoren. Et eksempel er beregning av størrelsen på et barnebidrag, der relevante rettskilder er fortolket og gitt en egnet representasjon i saksbe-

[18] Minstekrav til innhold i pasientjournal er angitt i pasientjournalforskriften, 21. desember 2000 nr. 1385 § 8.

[19] Et viktig aspekt ved representasjoner er at de er kvalitativt forskjellige fra det som representeres, samtidig som de anerkjennes som en gyldig og egnet gjengivelse. Et interessant filosofisk blikk på representasjoner finnes i Marx W. Wartofsky (1979): *Models: representation and the scientific understanding*. Han argumenterer for at hva som helst i utgangspunktet kan være en representasjon av hva som helst annet, det som gjør noe til en representasjon er at det blir tatt for å være det. En representasjonen er ikke bare en nøytral avbildning, den vil også i seg selv kunne være meningsbærende og overskridende (introduksjonskapitlet, særlig s. xx–xxi).

handlingssystemet. Svært ofte befinner man seg i en mellomposisjon, i den forstand at det kan være ønskelig eller nødvendig bare å representere deler av de rettslige normene i IT-systemet. De normene som da ikke inngår i IT-systemet blir naturligvis ikke borte, de må like fullt ivaretas i virksomheten.[20] De normene som regulerer berettigelsen av tilgang til og videreformidling av helseopplysninger vil et langt stykke på vei kunne uttrykkes som representasjoner i de aktuelle IT-systemene. Det er imidlertid mer tvilsomt om det er mulig, og i så fall ønskelig, å oppnå en fullstendig rendyrket teknologisk representasjon av denne reguleringen.

2.1.1 Rettsteknologi som forskningsfelt

Rettsteknologi er en vid betegnelse for teknologi som i en eller annen form inneholder rettslig materiale. Begrepet rettsteknologi er en slags samlebetegnelse for noen forskningstemaer, det har ikke et skarpt avgrenset innhold. Det kan både dreie seg om å gjøre rettskildestoff tilgjengelig, og om å representere normer slik at de i en eller annen form simulerer eller utfører rettslige performativer. Ved Senter for rettsinformatikk er rettsteknologi definert slik at det omfatter tre delområder. Det første delområdet er teknologier for søking i og gjenfinning av rettskilder, det andre er transformering av rettskilder til datamaskinprogrammer, herunder også mer generelle studier av representasjon av rettsregler, mens det tredje er systemer for regelverksadministrasjon.[21]

Det som kan kalles rettsteknologiperspektivet i denne avhandlingen hører hjemme i det andre delområdet, transformering og representasjon av rettsregler. Teknologi som skal kontrollere databrukernes handlinger «håndhever», tvinger altså i en eller annen grad gjennom en etterlevelse av, de implementerte reglene. I internasjonal litteratur er det brukt ulike betegnelser om dette, blant de mer kjente er *Lex informatica,*[22] og det noe mer sjargongpregede *West coast code.*[23]

I dette delområdet av rettsteknologier kan man igjen grovt sett skille ut to tradisjoner. Den ene tradisjonen kan betegnes som forskning på avanserte metoder for representasjon av regler.

---

[20] Dette skillet mellom IT-systemers rettslige omgivelser og rettslige innhold er beskrevet grundigere og med et større utvalg av eksempler i Herbjørn Andresen (2008a): «Systemintegrasjon i e-forvaltningen og følgene for dokumentasjon av systemenes rettslige innhold». I: *Elektronisk forvaltning på norsk: Statlig og kommunal bruk av IKT*, s. 227–243. (s. 229).

[21] Senter for rettsinformatikk: «Forskningsområder, rettsteknologi»: *http://www.jus.uio.no/ifp/forskning/omrader/rettsinformatikk-og-eforvaltning/rettsteknologi/*.

[22] Joel R. Reidenberg (1998): «Lex informatica: The formulation of information policy rules through technology». I: *Texas Law Review,* s. 553–584.

[23] Lawrence Lessig (1999): *Code and other laws of cyberspace*. *West coast code* refererer til at teknologimiljøene, blant annet i «Silicon Valley» vest i USA, implementerer regulering som programkode i systemene. Det motsvarende begrepet *East coast code* brukes om mer tradisjonell juridisk virksomhet.

I rettsinformatisk litteratur hører blant annet retninger som kunnskapsbaserte systemer, rettslige ekspertsystemer og kunstig intelligens til i denne tradisjonen. Den andre tradisjonen kan betegnes som rettslig systemutvikling. Det er en mer pragmatisk tilnærming, med forskning som ligger betydelig nærmere bruksorganisasjonene og anvendt og utbredt teknologi. Innen denne tradisjonen går systemutviklingen hånd i hånd med utformingen av regelverket.[24]

2.1.2 Avanserte metoder for representasjon

Forskningen på avansert representasjon er den eldste av de to tradisjonene, og står for en betydelig andel av den vitenskapelige litteraturen innen rettsteknologi. Resultatene på dette området har primært vært av teoretisk art, og kanskje vel så viktige for sine bidrag til rettsfilosofi og normteori som til anvendt teknologi. De avanserte representasjonene kan ha helt forskjellige utgangspunkter og mål. For eksempel har forskere i noen tilfeller ønsket å fange inn et deontisk normsett så presist som mulig, mens andre har siktet mot å simulere rettslige resonnementer eller beslutningsprosesser.[25]

En underliggende premiss for avanserte representasjoner er at jussen ligger fast. Idealet er å fange inn og håndtere kompleksiteten i regelverket uten å endre eller fordreie innholdet i de regler eller prosesser som er representert.[26] Et ideelt kriterium for en god representasjon vil være at den ikke setter sine egne spor. Jo mer resultatet ligner det en god profesjonsutøver ville ha kommet frem til uten systemets hjelp, jo mer vellykket.[27] Det logiske målet er å utforske, og kanskje tøye grensene for, hva som kan representeres.

---

[24] Pionerartikkelen på feltet er Jon Bing (1977): «Automatiseringsvennlig lovgivning». I: *Tidsskrift for Rettsvitenskap,* s. 195–229, det er også videre bearbeidet i blant annet Jon Bing (1983): *EDB: mulighet og problem ved forenkling av regelverk*. Dette feltet var en del av motivasjonen bak Avdeling for forvaltningsinformatikk.

[25] Blant en rekke klassiske, og temmelig ambisiøse bidrag kan nevnes Trevor Bench-Capon og Marek Sergot (1988): «Towards a rule-based representation of open texture in law». I: *Computer power and legal language,* s. 39–61 og Kevin D. Ashley (1991): *Modeling Legal Arguments: Reasoning with Cases and Hypotheticals*. Det fines også enkelte arbeider fra norsk rettsinformatisk miljø på dette området, blant annet Henning Herrestad (1996): *Formal theories of rights* og Christen Krogh (1997): *Normative structures in natural and artificial systems*.

[26] Et eksempel som gir uttrykk for dette idealet er Thorne McCartys redegjørelse for sitt arbeid med dype begrepsmodeller: «The idea is to select a small set of these common sense categories, the ones that are most appropriate for a particular legal application, and then develop a knowledge representation language that faithfully mirrors the structure of this set. The language should be formal: it should have a compositional syntax, a precise semantics and a well-defined inference mechanism.» L. Thorne McCarty (1989): «A language for legal Discourse I. basic features» (konferanseartikkel).

[27] Dette kriteriet er beslektet med «Turing-testen» for kunstig intelligens, som er foreslått i Alan M. Turing (1950): «I.–Computing Machinery and Intelligence». I: *Mind,* s. 433–460. Testen er utformet som et tenkt imitasjonsspill, der en utspørrer skal avgjøre om den som svarer er maskin eller menneske. Poenget er ikke realismen i det tenkte spillet som sådan, men kriteriet om ikke å kunne skjelne mellom menneske og maskin. Turing-testen har vært omstridt, blant annet fordi kriteriet hevdes å redusere intelligens til et spørsmål om adferd. Uansett er det et kriterium som fremdeles plasserer intelligente maskiner et lite stykke inn i fremtiden.

Noe som kan ses om en slags mangel ved forskningen på avansert representasjon av rettsregler, selv om det for så vidt er en naturlig side ved denne typen forskningsinteresse, er at studiene har vært smalt orientert. De har stort sett bare dreid seg om selve representasjonen av det rettslige innholdet. Rettsinformatisk litteratur i denne tradisjonen knytter i liten grad regelrepresentasjonene til de organisatoriske, faglige og teknologiske omgivelsene de ville komme til å inngå i om de skal brukes i praksis.

Denne avhandlingens mest konkrete befatning med avanserte representasjoner som retts-teknologisk tradisjon er presentasjon og vurdering av elektroniske agenter for å håndtere kontroll med tilgang til og videreformidling av helseopplysninger.[28]

2.1.3 Rettslig systemutvikling

Den andre tradisjonen, innen det rettsteknologiske forskningsfeltet transformering og representasjon av rettsregler, er i større grad rettet mot sammenhenger mellom de normene som representeres i IT-systemet, og det organisatoriske og tekniske miljøet systemet skal virke i. Betegnelsen rettslig systemutvikling peker på samspillet mellom systemutviklingsfaget og det juridiske arbeidet med å tolke, konkretisere og detaljere regelverket som et sentralt element i dette forskningsfeltet. Utvalg av relevante rettskilder, tolkningsvalg og supplering av rettskildene er i seg selv er rettslige beslutninger.[29]

Til forskjell fra den teoriinteresserte forskningen på avanserte representasjoner, er rettslig systemutvikling praktisk og empirisk rettet. Det innebærer at normrepresentasjonene også ses i sammenheng med arbeidsprosessene, teknologiske omgivelser, og balansering av andre typer hensyn som politiske målsetninger, personopplysningsvern, ressursbruk, rimelige forventninger til databrukerens forkunnskaper med mer. I praktisk systemutvikling vil hensiktsmessige designvalg som oftest innebære standard teknologi og konvensjonelle måter å representere normene på. De mest fundamentale problemene innen avansert representasjon unngås, for eksempel vil det være mer nærliggende å fastlegge entydige kriterier for en regel enn å forsøke å modellere en kompleks gråsone eller rettslig skjønnsutøvelse. Imidlertid er det også grunn til å regne med, i hvert fall håpe, at de innsikter som vinnes gjennom forskning på avansert representasjon på sikt utvider repertoaret av representasjonsmåter i den konvensjonelle systemutviklingen.

---

[28] Kapittel 9.5.3 nedenfor. Enkelte elementer fra dette perspektivet er imidlertid også med i mer beskjedent omfang i noen av de øvrige prinsippene som presenteres og vurderes i avhandlingens kapittel 9.

[29] Se Dag Wiese Schartum (1993): *Rettssikkerhet og systemutvikling i offentlig forvaltning*, s. 10 og Dag Wiese Schartum (2005): *Utvikling av beslutningssystemer – fra lovtekst til programkode*, s. 8.

Under perspektivet rettslig systemutvikling er kriteriet for en god representasjon at den samlet sett er egnet til å håndtere en oppgave, og at resultatene er riktige målt mot de rettslige designbeslutningene. Det er ikke lenger et mål i seg selv at den jussen som representeres i IT-systemet må ligge fast. Tvert i mot kan det være ønskelig å bruke erfaringer høstet fra den rettslige systemutviklingen aktivt som en anledning til å forenkle og forbedre det bakenforliggende regelverket.[30] En tankevekkende side ved representasjon – uansett om perspektivet er avanserte representasjoner eller rettslig systemutvikling – er at samme regelverk vil kunne være opphav til flere ulike designvalg. I en sammenligning av rettsteknologiske designvalg er det derfor også betimelig å undersøke om noen valg tilgodeser eller overser interesser eller verdier som ligger i utkanten av det representerte regelverket.

I denne avhandlingen er rettslig systemutvikling det mest treffende perspektivet for de fleste av de teknologiske prinsippene som vurderes. Teknologistøtte for kontroll med databrukernes handlinger er representasjoner av den reguleringen som berettiger tilgang til og videreformidling av helseopplysninger. De forskjellige teknologiske prinsippene for kontroll er ulike valg av design og representasjonsmåte. Egnethetsvurderingen av de teknologiske prinsippene er en forsøksvis samlet vurdering av hvor godt resultat kontrollmetodene gir. Det omfatter naturligvis selve representasjonen av rettsreglene i kontrollsystemet, men vil også dreie seg om administrerbarhet, treffsikkerhet og mulighetene for å avdekke og reagere på feil. Ikke minst inngår sammenhenger mellom designvalg for kontrollmetodene og videre hensyn som personvern, informasjonssikkerhet og forsvarlige helsetjenester i en samlet vurdering.

2.2 Representasjonsstrategier og klassifisering av normer

Å utarbeide alternative representasjoner av rettsregler forutsetter at man tar hensyn til at det kan finnes ulike kategorier og nivåer av normer. Man kan tenke seg en nivåinndeling mellom det som er regler, og det som er formål, idealer eller hensyn reglene skal realisere. Et formål kan være uttrykt eksplisitt i rettskildene, men er det ikke nødvendigvis. Formål, idealer og hensyn er prinsipielt forskjellig fra reglene.[31] For eksempel hører pasientautonomi, person-

[30] Å tilbakeføre til regelverket de valg som treffes under design av systemer er et perspektiv som drøftes under betegnelsen «techno-regulations» i Roger Brownsword (2005): «Code, control, and choice: why East is East and West is West». I: *Legal Studies,* s. 1–21.

[31] En inndeling som skiller mellom disse nivåene er «the Realm of the Good», der verdier og hensyn hører hjemme, og «the Realm of the Ought» der prinsipper og regler hører hjemme, i Robert Alexy (2002): *A Theory of Constitutional Rights*, s. 93.

vern og rettssikkerhet til formålsnivået, mens de konkrete reglene er virkemidler som støtter, balanserer eller undergraver formålene. Noen ganger kan regler inneholde referanser til formålsformuleringer, slik at nivåinndelingen blir mindre skarp.[32] En regel som refererer til sin begrunnelse er like fullt en regel. Det skillet som er av betydning her er at det er regelnivået som er gjenstand for representasjon, mens formålsnivået kan tenkes som en målestokk for representasjonens kvalitet.

Det kan være forskjellige måter å dele inn regler på. En innflytelsesrik og omdiskutert inndeling er mellom primære og sekundære regler: «Rules of the first type impose duties; rules of the second type confer powers, public or private.»[33] Inndelingen innebærer en rangering. Sekundære regler beskrives som i en viss forstand parasittiske, de dreier seg om å introdusere, endre, tolke og håndheve primære regler.

En inndeling som både er mer hensiktsmessig til dette formålet og mer utbredt i norsk teori er de tre kategoriene pliktnormer, kompetansenormer og kvalifikasjonsnormer, uten noen uttrykt rangordning mellom kategoriene.[34] Pliktnormer sikter ikke bare til plikter i snever forstand, men til en rekke nyanser av rettslige plikter og rettigheter. Innen rettsinformatikken er det mer vanlig å bruke fremmedordet deontiske normer i stedet for pliktnormer, det er et synonym som dekker det samme.

Et både analytisk og praktisk interessant spørsmål i klassifiseringen av normer er hvorvidt normer av én kategori lar seg uttrykke som om de tilhørte en annen kategori. Det mest fristende eksemplet, for den som ønsker enkle representasjoner, ville være å redusere kompetansenormer til deontiske normer. Dersom det er mulig å omforme normer fra en kategori til en annen uten meningstap, betyr det at man egentlig kunne greie seg uten den omformbare kategorien. Den overflødige kategorien kan finne eksistensberettigelse i å være bedre egnet pedagogisk eller systematisk enn den kategorien den reduseres til, men den ville altså kunne unnværes når man designer representasjoner av normen. Påstanden her er at de normene og representasjonene som vurderes i denne avhandlingen ikke kan reduseres fra en kategori til en annen. Det er med andre ord en helt reell kompleksitet i regelverket.

Høy kompleksitet i regelverket innebærer ikke at avanserte representasjoner som fanger opp flest mulig aspekter ved reglene nødvendigvis fører til det beste resultatet samlet sett. Vurderingen av hva som er en hensiktsmessig representasjon må ses i sammenheng med de

[32] Et eksempel er setningsleddet «medmindre det lader sig forsvare holdt op imod Ytringsfrihedens Begrundelse i Sandhedssøgen, Demokrati og Individets frie Meningsdannelse», i Grunnloven, 17. mai 1814 § 100, der formålsnivået (begrunnelsene) er direkte referert i dette leddet av regelformuleringen.
[33] H. L. A. Hart (1961): *The Concept of Law*, s. 79.
[34] Denne inndelingen i kategorier er brukt flere steder, blant annet i Torstein Eckhoff og Nils Kristian Sundby (1991): *Rettssystemer: systemteoretisk innføring i rettsfilosofien*.

øvrige rettslige, teknologiske, administrative og faglige omgivelser. For eksempel kan en angivelse av hva som berettiger en handling være enklere å kontrollere i praksis dersom den er enkel å administrere, men upresis, enn en som bygger på et større spekter av betingelser som krever et mer omfattende ajourhold.

Et moment som kan være tungtveiende i praksis, men som likevel ikke forfølges spesielt i denne avhandlingen, er de føringene og bindingene som følger med valget av teknologisk plattform.[35] En virksomhet får en del muligheter for å kontrollere sine databrukere i de programvareproduktene de kjøper fra en leverandør. Noen av mulighetene i programvarens funksjonalitet dekker behovene godt, andre mindre godt.

2.2.1 Rettighetsrelasjoner som nyanseringer av plikter og rettigheter

Tidlig på 1900-tallet skrev den amerikanske juristen Hohfeld to artikler om begrepene plikter og rettigheter.[36] Hohfelds artikler har hatt stor innflytelse på to områder. Det første området er innen det som var hans eget ærend, en begrepsanalyse av rettigheter og plikter som skulle bidra til mer nyansert forståelse. Det andre området er den betydning Hohfelds skjemaer har hatt i utviklingen av teorier om formelle representasjoner av rettslig kunnskap.[37]

Den «etablerte sannhet» som Hohfeld argumenterte mot, var forestillingen om at plikter og rettigheter samtidig både var motsetninger, og var korrelert slik at en persons rettighet nødvendigvis motsvares av en annens plikt.[38] Hans nyansering hadde to elementer: For det første en mer finmasket inndeling av rettigheter og plikter, som fanget inn flere varianter av disse to begrepene. For det andre splittet han opp relasjonsegenskapene motsetning og korrelasjon, slik at samme begrepspar ikke lenger var begge deler samtidig. Resultatet var to skjemaer, det ene over motsatte begreper, det andre over korrelerte begreper.[39]

---

[35] Sammenhenger mellom representasjonsmuligheter og teknologisk plattform er drøftet i Herbjørn Andresen (1999): «Om samsvaret mellom et IT-system og et rettslig regelverk, systemdokumentasjon som viser til rettskilder», særlig s. 27–30 Selv om verken teknologien eller regelverket er direkte sammenlignbart, kan selve poengteringen av denne sammenhengen ha en viss overføringsverdi til denne avhandlingens problemstilling.

[36] Wesley Newcomb Hohfeld (1913): «Some Fundamental Legal Conceptions as Applied in Judicial Reasoning». I: *Yale Law Journal,* s. 16–59. Den andre artikkelen om samme tema ble publisert i samme tidsskrift i 1916. Alle henvisninger til Hohfeld i denne avhandlingen er fra 1913-artikkelen.

[37] En omtale av noen av disse tilnærmingene finnes i Andrew J. I. Jones og Marek Sergot (1992): «Deontic logic in the representation of law: Towards a methodology». I: *Artificial Intelligence and Law,* s. 45–64. Filosofen Stig Kanger trekkes der, og også ofte ellers, frem som «opphavsmann» til å bruke Hohfelds skjemaer som utgangspunkt for å representere rettslige plikter, rettigheter, tillatelser og forbud i en formell deontisk logikk.

[38] «One of the greatest hindrances to the clear understanding, the incisive statement, and the true solution of legal problems frequently arises from the express or tacit assumption that all legal relations may be reduced to 'rights' and 'duties'.» Hohfeld (1913), s. 28.

[39] Oversettelsen av ordene i skjemaene er basert på Eng (2007), noe som gir en stort sett hensiktsmessig tillempning til norske rettslige begreper. Helt uproblematiske er oversettelsene imidlertid ikke. Det norske ordet *avhengighet* er brukt som oversettelse for *liability*. I en tidligere dansk utleggelse av Hohfelds skjemaer er

Motsetninger

krav	frihet	kompetanse	immunitet
ikke-rettighet	plikt	inkompetanse	avhengighet

Korrelasjoner

krav	frihet	kompetanse	immunitet
plikt	ikke-rettighet	avhengighet	inkompetanse

Nyanseringen av plikt- og rettighetsbegrepene gir intuitivt rikere begreper for å representere rettsregler. Et eksempel som ligger nær avhandlingens problemstilling, men som foreløpig ikke fremsettes i presis form eller med referanser, er regulering av videreformidling av helseopplysninger gjennom unntak fra taushetsplikt. Noen slike unntaksbestemmelser er en krav-rettighet for mottakeren, som innebærer en plikt til å avgi opplysninger for den som er omfattet av unntaksbestemmelsen. Det finnes imidlertid andre typer unntak som gir frihet til å avgi opplysninger, altså noe man kan gjøre, og denne friheten korrelerer med en ikke-rettighet. Den som etter unntaksbestemmelsen kunne ha mottatt opplysninger har dermed ikke krav på å få dem. Sett fra avgiversiden er frihet og plikt motsetninger, slik det også fremgår av Hohfelds første skjema. Brukt på den måten tilfører skjemaene nyanser som kan bidra til mer presise beskrivelser av normative relasjoner mellom aktører.

Et viktig trekk ved skjemaene er at de trekker inn kompetanserelasjoner i det mer nyanserte bildet av plikter og rettigheter. Hohfeld viste, gjennom mange eksempler fra amerikansk rettspraksis på slutten 1800-tallet, og noe støtte i juridisk teori, at den upresise bruken av begrepene plikt og rettighet i en del tilfeller dreide seg om positiv og negativ handlingsevne i relasjoner mellom parter. Med andre ord, og overført til den klassifiseringen som er brukt her, viste han flere eksempler på at ordene plikt og rettighet ble brukt både om deontiske normer og om kompetansenormer.

Ettersom Hohfelds nyansering viste at den alminnelig utbredte bruken av ordene plikt og rettighet også rommet kompetansenormer, blir det nærmest noe ironisk ved deler av den berettigede kritikken mot bruken av skjemaene til å representere rettsregler i en formell deontisk logikk. I noen av de tidlige forsøkene gikk en stor del av nyanseringen tapt nettopp fordi man forsøkte å redusere kompetansenormene til deontiske normer.[40] Ulike senere bidrag

---

samme ord oversatt med *underkastelse,* riktignok med en bemerkning om at «Sprogligt kan det være lidt vanskelig at operere med dette udtryk, fordi det har ensidig 'ufordelagtigt' præg, men også skal dække modstykket til fordelagtige dispositioner.» Alf Ross (1953): *Om ret og retfærdighed: en indførelse i den analytiske retsfilosofi*, s. 203.

[40] Denne kritikken er reist og begrunnet utførlig i David Makinson (1986): «On the formal representation of rights relations». I: *Journal of philosophical Logic,* s. 403–425.

til formell representasjon av rettigheter og plikter har både drøftet behov for ytterlig presiseringer av Hohfelds begreper, og behov for mer detaljerte logiske formalismer å representere begrepene med.[41]

2.2.2 Eliminasjon og konstruksjon som representasjonsstrategier

Rettslige begreper er ord og uttrykk som begrepsbrukeren forstår på bestemte måter når de inngår i en rettsregel eller et rettslig resonnement. Et slags tolkningsmessig utgangspunkt vil ofte være å basere forståelsen på en alminnelig dagligtalebetydning, men begreper får raskt faglige valører. Det finnes ulike teorier og perspektiver på hva rettslige begreper egentlig er. To forskjellige perspektiver er særlig interessante å sammenligne her, fordi de på hver sin måte får konsekvenser for hva som vil være hensiktsmessige og egnede representasjoner.[42]

Det ene perspektivet er at rettslige begreper utledes fra de rettsreglene som de inngår i. Meningsinnholdet i et rettslig begrep er da i prinsippet intet mindre, men heller ikke mer, enn alle holdbare slutninger fra regler der det aktuelle begrepet inngår.[43] Teorien om rettslige begreper som koblingsord, som særlig den danske teoretikeren Alf Ross forfektet, hviler nokså tungt på at meningen bestemmes av slutningene. Et rettslig begrep kan ses som en term som ligger mellom et sett betingelser og virkninger, og som forenkler forbindelsene mellom dem. For eksempel kan man betrakte forvaltningslovens legaldefinerte begrep «enkeltvedtak» som et koblingsord.[44] Visse kriterier må oppfylles for at noe skal være et enkeltvedtak, og dersom kriteriene er oppfylt utløser det visse virkninger. En moderat forståelse av koblingsordteorien vil være at enkeltvedtak er et rettslig begrep som fungerer som en mellomliggende term som systematiserer og forenkler forbindelsene. Det er likevel rom for, etter denne moderate forståelsen, å knytte noe selvstendig betydningsinnhold til begrepene. For eksempel kan det være hensiktsmessig for et forvaltningsorgan å bruke ordet enkeltvedtak i et svar på en søknad, ikke bare som en forenkling for å spare inn noen setninger om hva det innebærer, men kanskje også for på den måten å signalisere at de vedkjenner seg den tilhørende katalogen over prosessuelle virkninger av at noe er et enkeltvedtak.

---

[41] Noen eksempler på dette kan finnes blant annet i Jones og Sergot (1992), og i Lars Lindahl (2005): «Hohfeld relations and spielraum for action». I: *Studier i rättsekonomi. Festskrift till Ingemar Ståhl*, s. 121–150.

[42] Fremstillingen av disse to perspektivene er i høy grad basert på to artikler: Lars Lindahl (2004): «Deduction and Justification in the Law. The Role of Legal Terms and Concepts». I: *Ratio Juris,* s. 182–202 og Giovanni Sartor (2009): «Legal concepts as inferential nodes and ontological categories». I: *Artificial Intelligence and Law,* s. 217–251.

[43] Sartor (2009), s. 220.

[44] «[I denne lov menes med:] enkeltvedtak, et vedtak som gjelder rettigheter eller plikter til en eller flere bestemte personer;» forvaltningsloven, 10. februar 1967 § 2(1)(b).

Koblingsordteorien har imidlertid også en mer radikal side, og det er den som har spesiell betydning for hvordan rettsregler kan representeres. Dersom koblingsordet bare er en forbindelse mellom betingelser og virkninger, og ingenting annet, er det strengt tatt overflødig. Som et alternativ til å la begrepet «enkeltvedtak» administrere forbindelser mellom ett sett av betingelser og et annet sett av virkninger, kan man heller velge å spesifisere hver enkelt forbindelse mellom hver av betingelsene og hver av virkningene. Dermed er koblingsordene, ut fra den radikale forståelsen, eliminerbare.[45] Antallet forbindelser kan selvfølgelig bli høyt og uoversiktlig, og mangle systematisk eleganse, men dersom rettslige begreper er eliminerbare koblingsord vil altså meningsinnholdet være det samme.

I den moderate forståelsen av koblingsordteorien vil man ikke nødvendigvis betrakte et koblingsord som fullstendig eliminerbart. I det lille eksemplet ovenfor har forvaltningsorganet brukt ordet enkeltvedtak for å signalisere erkjennelsen av en forpliktelse. Avhengig av hvor mye man skal legge i det å signalisere, er det mulig å se for seg at dette kan føre til at koblingsordet «enkeltvedtak» begynner å leve sitt eget liv og pådrar seg selvstendige egenskaper. Dermed er det ikke lenger like sikkert at koblingsordene kan elimineres uten å tape meningsinnhold. Koblingsord kan slutte å være eliminerbare ved at de i praksis brukes på måter som forhindrer eliminasjon. Referanser til koblingsord i nåtidig norsk rettsteori er i hovedsak basert på denne moderate forståelsen.[46]

Den radikale forståelsen ligner en hel del på uttrykket reduserbarhet, som er brukt ovenfor om det å omskrive normer fra én kategori til en annen uten å tape mening. Eliminasjon av et koblingsord er å omskrive til en uttømmende liste over forbindelser, men innenfor samme normkategori. Dersom man velger å akseptere at koblingsord er eliminerbare, åpner det for flere og mer fleksible måter å representere de rettslige begrepene på i et informasjonssystem.

Et eksempel som vil være relevant for problemstillingen er angivelsen av hvilke opplysninger helsepersonell kan videreformidle om en pasient. I helsepersonellovens hovedbestemmelse om taushetsplikt er kriteriene angitt i nokså generelle termer.[47] Enkelte andre bestemmelser i helsepersonelloven henviser indirekte til samme angivelse gjennom begrepet «taushetsbelagte opplysninger».[48] Hvis det er slik at koblingsordet taushetsbelagt kan elimineres, åpner det for representasjoner som omgår dette begrepet ved å finne andre måter å fange opp

[45] Alf Ross' kostelige artikkel om en fiktiv sosialantropologs forskning på tabuer er en offensiv og pedagogisk polemikk om koblingsordenes eliminerbarhet. Alf Ross (1957): «Tû-tû». I: *Harvard Law Review,* s. 812–825.
[46] Jf. for eksempel betraktningen om at det er et rettslig spørsmål *i hvilken grad* et ord er et koblingsord, i Eng (2007), s. 107.
[47] Formuleringen i helsepersonelloven, 2. juli 1999 nr. 64 § 21, er «opplysninger om folks legems- eller sykdomsforhold eller andre personlige forhold.»
[48] For eksempel adgang til å gi taushetsbelagte opplysninger videre til samarbeidende helsepersonell, § 25(1), eller hjemmel til å gi forskrift om bruk av taushetsbelagte opplysninger i forskning § 29(3).

de forbindelsene mellom kriteriene og virkningene som det er behov for. Det utelukker selvfølgelig ikke at man også kan velge å representere koblingsordet mer direkte dersom det er mest hensiktsmessig, for eksempel gjennom en informasjonsmodell der «taushetsbelagt» er en egenskap som tilordnes de opplysningene dette gjelder.

Denne avhandlingen forutsetter ikke at koblingsord generelt og allmenngyldig må være eliminerbare, det er altså den moderate forståelsen som er utgangspunktet. Likevel er det under perspektivet rettslig systemutvikling rom for å undersøke, for hvert konkrete rettslige begrep, om det kan elimineres eller ikke. Det skulle være uproblematisk å omgå koblingsordet taushetsbelagt, i hvert fall ut fra de begrensede henvisningene som er gitt her, ved å velge alternative representasjonsmåter.

Det andre perspektivet er at begreper defineres, bestemmes eller konstrueres ut fra en intensjon om å *fastlegge* begrepets betydning og relasjon til andre begreper. En betegnelse som særlig brukes innen rettsinformatikk er rettslige ontologier, selv om en rettslig ontologi i utgangspunktet ikke trenger å ha noe med teknologi å gjøre. Det er en systematisk ordning av beslektede begreper, som regel i hierarkier med overordnede og underordnede begreper, gjerne i flere ledd. En ontologi gir rom for at teoretiske begreper kan ha en mindre direkte forankring i rettskildene enn det som er tilfellet med koblingsord. Et begrep, eller en hierarkisk relasjon mellom begreper, er ikke nødvendigvis bare utledet av eksisterende rettsregler. I visse tilfeller kan begreper konstrueres for ontologiens indre sammenhengs skyld. Dersom man ønsker at ontologien skal være systematisk dekkende for et formål, kan det være rom for å danne utfyllende begreper som enten bare finnes som antiteser til andre begreper eller som det er vanskelig å finne annet belegg for enn at de er nødvendige for å utfylle systematikken. En ontologiorientert forståelse av rettslige begreper er nærliggende innen rettslig systemutvikling. Transformeringen av rettsregler til programkode vil ofte være noe annet og mer enn en nøytral alternativ representasjon, teorien på området vektlegger også utvalg og supplering av rettskildene som en side ved det juridiske tolkningsarbeidet.[49]

Et eksempel som ligger nær problemstillingen er pasientens samtykke som et berettigende grunnlag for å videreformidle helseopplysninger.[50] I en ontologi vil samtykke som sådan befinne seg relativt høyt i hierarkiet, mens for eksempel samtykkets form og rekkevidde med mer befinner seg noe nedenfor. Enda lenger ned i hierarkiet, formodentlig, kan det tenkes et

[49] Jf. Schartum (1993), s. 148.
[50] Her er dette eksemplet bare en spinkel illustrasjon, og ikke på noen måte fyllestgjørende. Samtykke til behandling av helseopplysninger er drøftet nærmere i avhandlingens kapittel 6.

behov for noen begreper om tilbaketrekking av samtykke.[51] Tilbaketrekkingen er det kanskje hensiktsmessig å knytte sammen med noen andre praktiske hensyn, eksempelvis ved å plassere «robust administrasjon av samtykke» som et felles begrep ovenfor i hierarkiet. Robust administrasjon, i dette lille eksemplet, vil knapt kunne kalles noe rettslig begrep. Det fungerer snarere som en plassholder, eller spredningsnode, i den systematiske ontologien.

I de senere år har ordet ontologi fått stor utbredelse innen informatikken.[52] Det betegner en formalisert struktur av begreper, med en systematikk som er innbyrdes overensstemmende og entydig. Et begrep i ontologien skal ideelt sett ha de samme egenskapene uavhengig av hvilken løype man følger gjennom strukturen for å finne frem til det. Ontologier har særlig fått stor betydning innen heterogene systemer der felles begreper og opplysninger deles mellom forskjellige virksomhetsinterne og eksterne brukere, prosesser og delsystemer. Behovet og ambisjonen er semantisk interoperabilitet,[53] som innebærer at informasjonen er organisert slik at den bevarer et felles og konsistent meningsinnhold når den hentes frem, tolkes og behandles på tvers av teknologiske miljøer og brukssituasjoner.

Å betrakte rettslige begreper som koblingsord eller som ontologiske kategorier er to perspektiver blant flere mulige. Disse perspektivene lever godt side om side, og begge beriker mulighetene for formaliserte representasjoner. Begrensningene og fallgruvene må man imidlertid også være oppmerksom på.

Ettersom koblingsord er utledet fra rettsreglene de inngår i, vil meningsinnholdet endre seg i små skritt når bruken utvides eller innsnevres. Dersom man på ett tidspunkt har kommet til at «taushetsbelagte opplysninger» kan behandles som et eliminerbart koblingsord, har man likevel ingen garanti for at denne vurderingen holder vann over tid. Endret bruk av begrepet, for eksempel i retning av mer performativ fastlegging av hva som skal være taushetsbelagt, kan føre til at grunnlaget for den tidligere vurderingen blir gradvis endret.

Ontologier er konstruert med bakgrunn i en analyse. Når en ontologi skal utarbeides, kan begrepsstrukturens innretning og generaliseringsnivå tilrettelegges for å absorbere påregnelige

[51] I de fleste tilfeller er ikke tilbaketrekking regulert eksplisitt, unntaket er samtykke til medisinsk og helsefaglig forskning, der det er innført en egen bestemmelse om tilbaketrekking av samtykke og hvilke virkninger dette skal ha, jf. helseforskningsloven, 20. juni 2008 nr. 44 § 16.

[52] Ontologi betyr «lære om det værende», og er et ord med opprinnelse i filosofien. Den moderne informatiske betydningen er mer konsis og avgrenset. Følgende informatiske definisjon er ofte sitert: «An ontology models the vocabulary and meaning of domains of interest: the objects (things) in domains; the relationships among those things; the properties, functions, and processes involving those things; and constraints on and rules about those things.» Michael C. Daconta m. fl. (2003): *The Semantic Web: a guide to the future of XML, Web services, and knowledge management*, s. 190.

[53] I et slikt heterogent miljø, i nyere terminologi omtalt som *semantisk web*, er det i prinsippet bare informasjonen, og ikke de teknologiske og organisatoriske omgivelsene, som binder helheten sammen. Jf. Thale Omveien (2010): *Tribus Lingua – håndbok i teknokratsjargong*.

endringer i begrepsbruken. Man kan for eksempel se for seg et knippe nye og detaljerte regler om tilbaketrekking av samtykke, med ulike virkninger i ulike situasjoner. Hvis begrepsstrukturen er passe detaljert, men ikke altfor stram, er det godt håp om at de nye reglene kan innpasses i ontologiens allerede definerte begrep «tilbaketrekking», på samme plass i hierarkiet. Ontologiperspektivet kan derfor tilby mindre problematisk håndtering av små, skrittvise endringer enn utledningsperspektivet. På den annen side er selve strukturen i en ontologi mer statisk. Når endringene blir større enn ontologien er tilrettelagt for, blir det behov for en mer omfattende revisjon.

2.2.3 Selvregulering og handlingsrom som representasjonsproblem

De reguleringene som berettiger tilgang til og videreformidling av helseopplysninger er til dels, men ikke bare, generelle og kontekstuavhengige deontiske normer. Her brukes betegnelsen kontekstuavhengig om normer som er slik at det samme konkrete spørsmålet om berettigelse ideelt sett vil få det samme svaret uavhengig av hvilken virksomhet eller brukssituasjon spørsmålet oppstår i. Det enkleste, og likevel mest omfattende, eksemplet er helsepersonells taushetsplikt. Et spørsmål som gjelder taushetsplikten skal prinsipielt ha samme svar i sykehus A som i sykehus B. Motstykket er normer som gir den enkelte virksomhet som behandler helseopplysninger et så omfattende handlingsrom at det samme spørsmålet om berettigelse har flere ulike svar som er like holdbare.[54] For eksempel vil et spørsmål om hvilke opplysninger sykepleiere gis tilgang til i pasientjournalsystemet kunne få ulike svar i sykehus A og sykehus B, fordi dette er regulert av informasjonssikkerhetsbestemmelsene,[55] som legger opp til at hver av virksomhetene vurderer selvstendig hvilken risiko opplysningene er utsatt for og hva som samlet sett vil være de best egnede tiltakene for å avhjelpe sikkerhetsrisikoen.

Bakteppet for virksomhetenes handlingsrom er en høy grad av institusjonell autonomi som et grunnleggende utgangspunkt, som likevel begrenses gjennom betydelige innslag av politisk, rettslig og faglig styring og normering for å ivareta ulike samfunnshensyn. De hensynene som i særlig grad har betydning for avhandlingens emne er informasjonssikkerhet og personopplysningsvern, men disse kan ikke betraktes helt løsrevet fra andre hensyn de

[54] Foreløpig er ikke disse begrepene spesielt presise. Virksomheters handlingsrom er i denne sammenheng noe litt annet enn det som tradisjonelt betegnes som et rom for juridisk skjønn, selv om begrepene naturligvis også har en del til felles. Avhandlingens kapittel 4 dreier seg om å gi et bredt fundert belegg for hva denne typen handlingsrom for en virksomhet innebærer. I kapittel 6 drøftes både kontekstuavhengige regler og reguleringen av virksomheters handlingsrom som har betydning for tilgang til og videreformidling av helseopplysninger.

[55] Innenfor helsetjenesten og helseforvaltningen dreier dette seg om helseregisterloven § 16 og personopplysningsforskriften, 15. desember 2000 nr. 1265, særlig §§ 2-3, 2-4, 2-8, 2-11 og 2-14.

kommer i berøring med, som for eksempel pasientsikkerhet, samfunnskontroll, forskning eller arbeidstakeres ve og vel. Den rettslige og faglige normeringen er på mange områder basert på en form for offentligrettslig regulert selvregulering.[56] Det handlingsrommet en virksomhet får gjennom et selvreguleringsregime er imidlertid ikke en aksept for å vente og se, og så ta tak i problemer først når de dukker opp, eller for å la den enkelte ansatte gjøre som han eller hun selv synes er best. Selvregulering av dette slaget er en plikt virksomheten har til å fastlegge hvordan de skal ivareta det aktuelle samfunnshensynet. De regler, rutiner og kontrollaktiviteter som virksomheten selv bestemmer seg for å gjøre gjeldende skal kunne dokumenteres overfor, og etterprøves av, et eksternt tilsynsorgan.

Det handlingsrommet som premissgivere gir virksomheter gjennom selvregulering innebærer ikke på noen måte et fravær av rettslig og faglig normering.[57] Først og fremst har virksomhetene en plikt til å arbeide systematisk med normering og kontroll innad. Samtidig er det også en overføring av kompetanse, der premissgivere gir virksomheten tillatelse til å sette normene selv, innen visse rammer. Nedenstående betraktning, om hva den som gir tillatelse egentlig gjør, peker på en slik sammenheng mellom tillatelser og handlingsrom:

> Giving permission is a kind of «binding one's hands». It is somewhat like giving a promise or like saying «you are free to do this, I am not going to interfere». One could also say that the permission-giver imposes a prohibition on himself not to prevent the permission-holder from availing himself of the permission.[58]

En mulig strategi for å representere regler som er underlagt et selvreguleringsregime, er å ta utgangspunkt i relasjonen mellom premissgiver og virksomhet. Det er i så fall innholdet i og omfanget av den kompetansen virksomheten er tildelt, og dermed den ytre rammen som trekker grensene for handlingsrommet, som skal representeres i IT-systemet. Noen tilnærminger til denne typen representasjoner finnes i litteraturen. Blant de representasjonsmåtene som har vært foreslått er formaliserte uttrykk for at en virksomhet eller en del av en virksomhet har en plikt til å sørge for at en bestemt normativ tilstand er oppfylt. En slik tilstand kan for eksempel være at opplysninger om en pasient ikke er gitt til noen utenfor virksomheten uten holdbar berettigelse. I forlengelsen av plikten til å sørge for dette, kan virksomheten

[56] Dette er i utgangspunktet en relativt stor klasse av reguleringsmetoder, som finnes i mange varianter og under ulike betegnelser i internasjonal litteratur. Den formen for plikt til selvregulering som i første rekke definerer, og begrenser, virksomheters handlingsrom innen de samfunnshensynene som er relevante i denne avhandlingen kan betegnes som risikobasert internkontroll, jf. kapittel 4.

[57] «Premissgivere» er en aktørkategori som her brukes om lovgiver, fagmyndigheter, tilsynsorganer og standardiseringsorganer med videre som gir rammer for behandling av helseopplysninger, uten at de selv behandler slike opplysninger i nevneverdig omfang. Det er gjort noe nærmere rede for kategorien premissgivere i kapittel 3.4.

[58] Georg Henrik von Wright (1999): «Deontic Logic: A Personal View». I: *Ratio Juris,* s. 26–38. (s. 37).

definere at visse handlinger skal regnes som midler til å opprette visse normative tilstander.[59] Representasjonene av hva virksomheten må sørge for, er formelle uttrykk for den plikten en virksomhet har til å fastlegge hvordan samfunnshensynet skal ivaretas, med de rammer og standarder virksomheten må holde seg innenfor. Dette leddet i representasjonen er altså samfunnets «ytre krav» til virksomheten.[60] Representasjoner av hva som skal regnes som oppfyllelse av kravene er uttrykk for det interne arbeidet i virksomheten. Det omfatter både beslutninger, gjennom det å utarbeide representasjoner innenfor handlingsrommet, og etterlevelse ved å bruke disse representasjonene.

En nærliggende og pragmatisk representasjonsstrategi, som også er det som hovedsakelig gjøres i praksis, er å la være å utarbeide representasjoner av samfunnets ytre krav. Denne strategien innebærer at det ikke blir etablert felles, formaliserte representasjoner, som kan brukes gjennomgående på tvers av IT-systemer og virksomheter. For de delene av regelverket som er basert på selvregulering, der virksomhetene har et betydelig handlingsrom, må det også nødvendigvis være slik. Konsekvensen er imidlertid at også kontekstuavhengige deler av reguleringen, som bør fungere mest mulig likt på tvers, transformeres til forskjellige representasjoner i de enkelte virksomhetene. Så lenge helseopplysninger holdes innenfor en virksomhet er mangelen på felles representasjoner et relativt lite problem. Det vil med stor sannsynlighet føre til enkelte forskjeller i måten sykehus A og sykehus B håndterer regler om behandling av helseopplysninger på, også der det ideelt sett ikke skulle ha vært noen forskjell. Som en liten spissformulering kan det sies at mangelen på felles representasjoner av samfunnets ytre krav overlater så mye til virksomhetene at de i praksis har et enda større handlingsrom enn det de strengt tatt har fått tildelt gjennom selvreguleringsregimet.

Felles representasjoner av samfunnets ytre krav gir teknologi som, i større grad enn lokale representasjoner, ivaretar felles tolkninger kontekstuavhengige regler. Det å etablere og å vedlikeholde slike felles representasjoner er imidlertid ikke problemfritt. For det første fører det med seg økt teknologisk kompleksitet, som både kan gjøre systemer mindre kostnadseffektive og øke risikoen for omgåelser. For det andre vil det føre til at den formelle rigiditeten som preger deler av de kontekstuavhengige reglene tvinges gjennom, kanskje i unødvendig høy grad, i de felles representasjonene. For det tredje blir det vanskeligere å forutsi omfang og

[59] Denne todelingen av hvordan man kan representere kompetanse og oppfyllelse av tildelt kompetanse er en forenkling, om ikke det skal kalles en vulgarisering, av Andrew J. I. Jones og Marek Sergot (1996): «A Formal Characterisation of Institutionalised Power». I: *Logic Journal of the IGPL,* s. 427–443. (s. 430–431).

[60] I regulatorisk forstand betyr «representasjoner av samfunnets ytre krav» et element av sentralisert tolkning og design, som gjøres gjeldende på tvers av virksomhetsgrenser og ulike fysiske systemmiljøer. Det trenger imidlertid ikke nødvendigvis innebære sentralisering av teknologiske komponenter. Felles representasjoner innebærer ikke bestemte krav til måten å utplassere representasjonene på.

konsekvenser av endringer i regelverket. Endringer i felles representasjoner må iverksettes både i representasjonene av samfunnets ytre krav og i samvirket mellom de felles representasjonene og de lokalt forankrede representasjonene som virksomheten rår over selv.

Alternativet til felles formaliserte representasjoner av de ytre kravene, når helseopplysninger skal utveksles og brukes på tvers, er organisatoriske tiltak for å harmonisere rettslig og faglig normering til et felles og etterprøvbart nivå. Det er forskjellige måter å oppnå dette på. I praksis har det dreid seg om bilaterale avtaler mellom samhandlende virksomheter,[61] en viss grad av felles detaljering av faglige normer for informasjonssikkerhet innen sektoren,[62] eller ensretting av praksis gjennom oppfølgingen fra statlige tilsynsorganer som kan skaffe seg kunnskap om situasjonen i ulike virksomheter.

Kontroll med helseopplysninger, i horisontal samhandling mellom virksomheter, vil være vanskelig og innsatskrevende uansett om hovedstrategien er felles teknologiske representasjoner eller organisatorisk harmonisering. Kombinasjoner er også mulig, det er ikke nødvendigvis et enten-eller. Organisatorisk harmonisering, gjennom faglig normering og krav til avtaler, er den strategien som er mest synlig i rettskildene. Det kan forstås dit hen at organisatorisk harmonisering er foretrukket, men det kan også tolkes slik at organisatorisk harmonisering er å betrakte som et minstekrav, som må innfris dersom man ikke vil eller ikke lykkes med å ivareta kontrollen gjennom teknologiske representasjoner. Enkelte av de foreslåtte teknologiske kontrollprinsippene, som vurderes i avhandlingens del III, forutsetter på ulike måter visse felles formaliserte representasjoner av samfunnets ytre krav.

2.3 Tilgangskontroll som teknologisk disiplin

Begrepet tilgangskontroll dekker både selve teknologien som styrer hvem som skal få tilgang til å se, endre, formidle og ellers håndtere opplysninger, og virksomheters anvendelse av denne teknologien. Tilgangskontroll er ikke et rent teknologisk anliggende, det inngår som ett av flere elementer i virksomheters arbeid med informasjonssikkerhet, og omfatter blant annet avveininger mellom funksjonalitet og sikkerhet, fysiske omgivelser, virksomhetskultur, sanksjonsmuligheter og etikk, i tillegg til organisering og teknologi.

Den teknologiske siden av tilgangskontroll er i denne sammenheng en betegnelse som omfatter teorier, prinsipper, begreper og mer konkrete metoder og verktøy for å uttrykke,

[61] Jf. personopplysningsforskriften § 2-15.
[62] Jf. sikkerhetsnormen: «Norm for informasjonssikkerhet i helsesektoren», 7. august 2006.

håndheve og etterprøve databrukeres handlingsmuligheter i IT-systemer. Teknologier for tilgangskontroll vil i en eller annen grad tvinge gjennom de beslutningene om handlingsmuligheter som er truffet, og som er formelt representert i tilgangskontrollsystemet. Forsøk på å få lese eller bruke opplysninger i strid med tildelte tilgangsmuligheter skal ideelt sett avvises.

Avhandlingens hovedtittel, *tilgang til og videreformidling av helseopplysninger*, gir grunn til å spørre om tilgangskontroll som teknologisk disiplin også omfatter videreformidling. Det generelle svaret er ja, videreformidling er en av flere måter å bruke opplysninger på, og teknologier for tilgangskontroll omfatter kontroll med flere handlingsmuligheter enn bare lesing. En viss nyansering er likevel nødvendig: I noen tilfeller gir teknologien eksplisitte muligheter for å uttrykke krav til kontroll med videreformidling, i andre tilfeller vil det å kunne videreformidle opplysninger følge indirekte av andre måter å uttrykke handlingsmulighetene på.

2.3.1 Hovedaktivitetene innen tilgangskontroll

En utbredt klassifisering av hovedbegreper innen tilgangskontroll som informatisk disiplin er en inndeling i fire overordnede aktiviteter: Administrasjon, autentisering, autorisasjon og revisjon.[63] Alle de fire aktivitetstypene kan utøves både med og uten teknologiske verktøy, i praksis vil det ofte være en kombinasjon av manuelle rutiner og teknologi. Hvor god samlet kontroll en virksomhet har med tilgang til informasjon, avhenger av samspillet mellom alle de fire aktivitetene.

Administrasjon er rutinene og det praktiske arbeidet med å tildele, endre og trekke tilbake databrukeres handlingsmuligheter. Det omfatter også arbeidet med å definere og endre hvilke handlingsmuligheter som skal kunne tildeles. Teknologisk støtte for administrasjon kan bidra til å gjøre tilgangskontrollen administrasjonsvennlig og pålitelig. Tradisjonell administrasjon av databrukere innenfor ett og samme IT-system, innen en virksomhet, er relativt enkelt og vil normalt ikke være avhengig av avansert teknologisk støtte. Kompleksiteten stiger vesentlig når en felles forvaltning av identifikatorer og handlingsmuligheter skal favne tilgang til flere IT-systemer. Administrasjon av entydig identifiserte databrukere og konsekvent tildeling av handlingsmuligheter, i store og fragmenterte virksomheter eller på tvers av virksomheter, er langt fra trivielt.

[63] De engelske betegnelsene, *Administration, Authentication, Authorization* og *Audit*, omtales som «the four A's of Information Security». Roberta J. Witty m. fl., *Identity and Access Management Defined* (2003).

Autentisering er de teknologiske mekanismene som skal sørge for at en databruker er individuelt identifisert i IT-systemet, og gi tilstrekkelig sikkerhet for at vedkommende er den han eller hun gir seg ut for. En databruker kan autentiseres for systemet på ulike måter, den vanligste metoden så langt er og har vært et passord, som er unikt for den enkelte databrukers identifikator.

Etter hvert har alternativer til passord også begynt å bli utbredt. Passord er et eksempel på å autentiseres gjennom noe man vet. Å bruke et smartkort eller en annen fysisk gjenstand er å autentiseres gjennom noe man har, hvilket er en prinsipielt sterkere autentisering. Det kan sammenlignes med å bruke en fysisk nøkkel. Fingeravtrykk og andre biometriske data som kan brukes til å autentisere seg gjennom noe man er, er en enda sterkere autentisering som krever at personen må selv være fysisk tilstede.[64] For ytterligere å styrke autentiseringen, kan også to eller flere autentiseringsfaktorer kombineres. Et eksempel mange kjenner godt er bankkort, noe man har, som i de fleste situasjoner brukes i kombinasjon med en kode, noe man vet.

Hver av autentiseringsfaktorene kan realiseres på ulike måter, med forskjellige styrke-grader, mer eller mindre vellykket, og mer eller mindre faglig holdbart. Et passord kan gjøres vanskeligere å knekke ved å stille krav til dets lengde, krav til sammensetninger med ulike typer tegn, og krav til hvor ofte det må byttes. Et fingeravtrykk tilbyr i utgangspunktet en overbevisende forbindelse mellom en person og representert informasjon om personen, men gir likevel bare sterk autentisering når det inngår i en tilstrekkelig robust administrativ og teknologisk sammenheng. Autentiseringen er for eksempel ikke lenger like sterk dersom apparaturen ikke er i stand til å avsløre en falsk finger.[65]

Selv om administrasjon og autentisering er aktiviteter som har avgjørende betydning for tilgangskontrollens samlete kvalitet, er de ikke viet vesentlig oppmerksomhet i avhandlingen. Representasjoner av hva som berettiger tilgang til og videreformidling av helseopplysninger, og kontroll med at handlinger er berettigete, hører først og fremst til under aktiviteten autorisering. Aktiviteten revisjon, som innbefatter etterhåndskontroll med at databrukeres handlinger har vært berettigede, er også viet noe plass i avhandlingen.

[64] Denne inndelingen av autentisering gjennom faktorene «noe man vet», «noe man har» eller «noe man er» har lang historie. Eldste kilde jeg har lykkes å finne frem til er et foredrag av to forskere fra IBM i 1974, lenge før annen autentisering enn bruk av passord var aktuelt utover rent eksperimentelle sammenhenger. R. L. Thomas og Robert H. Courtney (1974): «A Systematic Approach to Data Security» (konferanseartikkel). Senere har en del teoretikere også føyd til en fjerde faktor, autentisering gjennom «noe man gjør».

[65] Gaurav S. Kc og Paul A. Karger, *Preventing Attacks on Machine Readable Travel Documents (MRTDs)* (2006).

Begrepet autorisasjon kan både brukes om de rettslig eller organisatorisk bestemte fullmaktene en person faktisk har, og om de tekniske mekanismene som sørger for samsvaret mellom personens fullmakter og handlingsmuligheter i IT-systemer. Den normative føringen er et best mulig samsvar mellom faktiske fullmakter og den tekniske representasjonen av disse fullmaktene, selv om et fullstendig samsvar er vanskelig å oppnå.[66] Aktiviteten autorisasjon dreier seg om (1) å beslutte hvilke kriterier som skal gjelde for at databrukere skal kunne tildeles en handlingsmulighet, (2) å utarbeide egnete representasjoner for de besluttede kriteriene, og (3) å sørge for at IT-systemene i rimelig grad tvinger gjennom de grensene som settes for en databrukeres handlingsmuligheter.

Revisjon skal i denne sammenhengen forstås relativt snevert, om etterhåndskontroll med databrukernes autorisasjon. Etterprøvingen skjer prinsipielt på to nivåer. Det ene nivået er hvorvidt en databruker har fått tildelt riktige handlingsmuligheter, altså om den representerte autorisasjonen er i overensstemmelse med besluttede kriterier. Det andre nivået er om vedkommende har handlet i samsvar med sine fullmakter.

2.3.2 Historisk bakgrunn for representasjoner av autorisasjon

Metoder for å holde informasjon hemmelig, og for å sikre at bare rette vedkommende fikk den i hende, har historie tilbake til oldtiden.[67] Mens helseopplysninger i tidligere tider utelukkende var beskyttet av legens taushetsplikt, har det på andre områder som militærvesen, politikk og handel alltid vært et visst behov for å kunne kommunisere fortrolig over avstand, og i situasjoner der tilliten ikke nødvendigvis er basert på personlige relasjoner.

Militære klassifiseringssystemer var det første området der det ble utarbeidet formelle prosesser og regler for håndtering av informasjon. Den grunnleggende metoden går ut på å klassifisere dokumenter og eventuelle andre gjenstander som bærer informasjonen, med ulike graderinger etter hvor sensitiv informasjonen er. De personene som skal kunne få tilgang til sensitiv informasjon blir klarert for en bestemt grad av sensitivitet. En klareringsmyndighet tar altså stilling til både hvilke informasjonsbehov en enkeltperson vil ha, og om vedkommende er tilstrekkelig skikket for å bli tiltrodd slik informasjon. Under Krimkrigen, årene 1853-1856, begynte det britiske militæret å merke dokumenter. Klassifiseringen var delt inn i tre nivåer, «Confidential», «Private Confidential» og «Secret and Confidential». Dette var

[66] De mest sentrale uttrykkene for den normative føringen følger i denne sammenhengen av helseregisterloven §§ 13 og 16.

[67] Et par fascinerende eksempler på paralleller mellom tidligere tiders og nåtidens problemer og løsninger på dette området er beskrevet i Jon Bing (1998): *Landskap med tegn: en liten bok om informasjonsteknologi og informasjonspolitikk*, s. 11–12.

starten på en praksis, men ingen andre elementer i et klassifiseringssystem var på plass på det tidspunktet. Det fantes verken regler for å håndtere dokumentene, klarering av mottakere eller sanksjoner ved overtredelse. Klassifiseringssystemet ble imidlertid utviklet videre i årene som fulgte, og i *Queen's Regulations and Orders for the Army* av 1868 var det gitt regler både om straff for ikke å følge krav til å beskytte informasjon, og begrensninger om at bare tiltrodde personer skulle kunne gis tilgang.[68]

Klassifiseringssystemer ble etter hvert supplert med et prinsipp om at man i tillegg til en formell klarering også skulle godtgjøre et reelt, tjenestelig behov for den informasjonen som man ønsket innsyn i. Dette prinsippet har neppe en like klar opprinnelse som kan tidfestes. En tidlig utgave var beskyttelsen av leveranser til britiske torpedoer, som allerede på 1880-tallet ble fordelt mellom flere leverandører slik at ingen private aktører skulle kunne lage en avansert torpedo.[69] Dette prinsippet om oppsplittet kunnskap var imidlertid ikke i utgangspunktet knyttet til klassifiseringsmodellen for informasjonskontroll.

Fra USA, i rutinene innenfor et militært forskningsmiljø, er følgende et relativt tidlig eksempel på at prinsippet om oppsplitting også ble et supplement til klassifiseringsmodellen for informasjonskontroll:

> Another step in the maintenance of security was that of compartmentalization of information. The Committee adopted as a guiding principle that no person associated with it desired to have or would be given any classified information except that needed for the performance of the particular tasks which had been entrusted to him.[70]

Erfaringene med dette prinsippet var ikke udelt positive, samme forfatter beretter at det ofte førte til tap av tid, og manglende helhetskunnskap. På den annen side antok man at den strenge sikkerhetspolitikken styrket det operative militærets tillit til forskningsmiljøet.

Prinsippet om oppsplittet kunnskap, og tilganger begrenset til det oppgaven krever, fikk etter hvert den mer velkjente betegnelsen «need to know»-prinsippet.[71] Senere har dette uttrykket blitt brukt som navn på et autorisasjonsprinsipp med bredere anvendelse enn som supplement til en klassifiseringsmodell. «Need to know» brukes også ofte som fagsjargong i

---

[68] Arvin S. Quist (2002): *Security Classification of Information: Introduction, History, and Adverse Impacts*, s. 15.
[69] Quist (2002), s. 16.
[70] Irvin Stewart (1948): *Organizing scientific research for war: The administrative history of the Office of Scientific Research and Development*, s. 28.
[71] Her siteres annenhånds fra en fotnote i en artikkel fra 1956, der dette fremgår av noe som den gang var nedfelt i det amerikanske utenriksdepartementets *Security Regulations* § 195.11(b): «No person is entitled to receive classified … information solely by virtue of his official position or by virtue of having been granted security clearance. The 'need to know' doctrine shall be enforced at all times.» Jf. Harold P. Green (1956): «Information Control and Atomic Power Development». I: *Law and Contemporary Problems,* s. 91–112. (s. 96, note 23).

norske tekster, uten oversettelse. I lover og forskrifter er imidlertid en norsk språkdrakt nødvendig. Leddet «… i den grad dette er nødvendig for vedkommendes arbeid …», i den setningen som er utgangspunkt for avhandlingens problemstilling, er et uttrykk for det samme autorisasjonsprinsippet.[72] Ellers er uttrykket «tjenestelig behov» en del brukt på norsk.

De tidligste teknologiske representasjonene av autorisasjon, var basert på klassifisering og klarering etter modell av militær informasjonskontroll.[73] Informasjonselementene, filer på en datamaskin eller forekomster i en database, fikk angitt en gradering som representerte et nivå i et hierarki over beskyttelsesbehov. Databrukerne var klarert for et bestemt nivå, som ga tilgang til informasjonselementer med samme eller lavere beskyttelsesbehov. Den representerte modellen var i realiteten den samme som ble utviklet under Krimkrigen. Den rommet ikke begreper om oppsplitting av kunnskap, og heller ingen representasjoner av godtgjorte behov for informasjonen. Dermed representerte denne modellen bare de formelle og statiske yttergrensene for autorisasjon. Den mer dynamiske siden, å avgrense tilganger i henhold til det reelle informasjonsbehovet, lå utenfor modellen og var overlatt til ikke-teknologiske tiltak som arbeid med sikkerhetskultur og reaktive sanksjoner.

Et stort fortrinn ved den ovennevnte Bell-LaPadula-modellen, og tilsvarende modeller for klassifisering og klarering, er at representasjonen av autorisasjoner ikke skiller mellom tilgang til og videreformidling av opplysninger. Både klassifiseringen av opplysningene og klareringen av databrukerne er universelle, og uavhengig av hvilke instanser som klassifiserer og klarerer. Dermed er det ingen forskjell mellom virksomhet A og virksomhet B, eller mellom IT-system X og IT-system Y. Det man selv har tilgang til er det i prinsippet trygt å videreformidle til alle som har iverksatt samme autorisasjonsmodell. Noe som nærmest kan virke litt paradoksalt er at mer sofistikerte autorisasjonsmodeller gjør forskjellene mellom å kontrollere tilgang og videreformidling større. Det skyldes at en mer presis autorisasjon i større grad bygger på lokale forutsetninger og beslutninger, og ikke er like universell som et klassifiseringssystem.

Det har senere kommet til mange ulike måter å representere databrukernes fullmakter på, for å dekke en rekke spesielle behov. Det er verken omfangsmessig mulig eller egentlig interessant å brette ut noen fullstendig historiske gjennomgang her. Et par eksempler kan likevel nevnes: I stedet for bare å kontrollere tilgang, rettes autorisasjonene mer mot å kontrollere mulige handlinger som endrer informasjonen. Et hyppig sitert begrep er oppgave-

[72] Helseregisterloven § 13(1) annet punktum.
[73] Den klassiske teoretiske modellen på dette området, oftest omtalt som *Bell-LaPadula*-modellen, og av og til omtalt som *the lattice model*, er presentert og begrunnet i D. Elliot Bell og Leonard J. LaPadula (1973): «Secure Computer Systems: Mathematical Foundations». I: *MITRE Technical Report 2547 vol. I*.

differensiering, for å styre arbeidsdeling mellom databrukere som har forskjellige oppgaver.[74] Senere introduseres prinsippet rollebasert tilgangskontroll, som skulle bli svært innflytelsesrikt.[75] Dette er både inspirert av behovet for å representere arbeidsdeling og andre fullmaktsforhold innenfor virksomheten, og av en praksis med å gruppere databrukere med samme tilgangsbehov for å forenkle administrasjonen. Det grunnleggende ved rollebasert tilgang er at autorisasjonen knyttes opp mot en rolle, i stedet for å knyttes direkte til den enkelte databruker. Autorisasjonen er indirekte i stedet for personlig. Komplekse modeller for rollebasert tilgang prøver også å ta opp i seg ulike måter tilganger struktureres på i en virksomhet, som delegasjon, fungering ved fravær og lignende. Noe av problemet med slike modeller er at ikke alle virksomheter følger samme politikk for hvorvidt for eksempel en leder automatisk skal ha samme tilganger som sine underordnede eller ikke. En rollebasert tilgangskontroll som gjøres mer sofistikert enn en ren gruppering av databrukerne vil ikke være universell.

Som en generell og sterkt forenklet betraktning, kan man si at utviklingen av måter å representere autorisasjon på følger to hovedspor. Det ene sporet er, som i eksemplet med rollebasert tilgang, å lage mer finmaskete representasjoner av de formelle og statiske ytter-grensene for autorisasjon. Jo bedre man lykkes, jo nærmere vil autorisasjonen ligge det man på forhånd har kunnet anta er det reelle informasjonsbehovet. Den statiske representasjonen innebærer likevel et fravær av mekanismer for å godtgjøre informasjonsbehovet eller å ta konkret stilling til det i en atypisk kontekst.

Det andre sporet i utviklingen er å representere dynamiske kriterier for autorisasjon. Det innebærer at databrukeren vil kunne støte på tekniske hindringer som skifter med ulike situasjoner, og med foranderlige egenskaper ved informasjonen. I utgangspunktet er dynamiske kriterier for autorisasjon det mest nærliggende for kontroll med helseopplysninger. Det som berettiger tilgang og videreformidling kan variere blant annet med hvor i et behandlingsforløp pasienten befinner seg, og med hva slags og hvor sterk medinnflytelse den enkelte pasient til en hver tid ønsker å utøve over behandlingen av opplysninger. I visse tilfeller forutsetter også berettiget tilgang og videreformidling at det treffes en konkret, skjønnsbasert beslutning.

Selv om dynamisk tilgangskontroll umiddelbart virker mest nærliggende for helseopplysninger, kan det likevel også forsterke enkelte problemer. Dynamiske kriterier, som skal

[74] Representasjoner av begrepet «separation of duties», med attestasjon og anvisning av regninger som standard-eksempel, er introdusert i David D. Clark og David R. Wilson (1987): «A Comparison of Commersial and Military Computer Security Policies» (konferanseartikkel).

[75] En tidlig artikkel om dette prinsippet er David F. Ferraiolo og D. Richard Kuhn (1992): «Role-Based Access Control» (konferanseartikkel). Det er verdt å merke seg hvordan tidlige vitenskapelige artikler om rollebasert tilgangskontroll selv beskriver begrepets historie: Det oppsto som pragmatiske praksiser ulike steder, og ble deretter fanget opp, formalisert og «vitenskapeliggjort» av miljøer som forsker på informasjonssikkerhet.

fungere automatisk i en gitt situasjon, vil forutsette at IT-systemet faktisk inneholder data som representerer den aktuelle situasjonen. Et eksempel kan være en henvisning fra fastlegen som grunnlag for at bestemte opplysninger gjøres tilgjengelig for ansatte ved en poliklinikk. Dette kriteriet fungerer bare så lenge henvisningen faktisk er registrert på en måte som gjenkjennes av tilgangskontrollsystemet. Det innebærer at kontrollen med tilganger i større grad blir avhengig av datakvaliteten. En slik forutsetning er likevel innenfor det som må anses som rimelig. Nytteverdien ville være mer tvilsom dersom helsepersonell blir nødt til å fabrikkere et høyt antall «på liksom»-situasjoner uten noen egentlig faglig begrunnelse, men som må være tilstede for å innfri dynamiske kriterier for autorisasjon. Et annet problem ved dynamiske kriterier, er at det kan være vanskeligere å oppnå sikkerhet mot omgåelser, altså uautoriserte handlinger, fra databrukernes side.[76] Blant de ulike autorisasjonsprinsippene som vurderes i kapittel 9 finnes det både statiske og noe mer dynamisk orienterte modeller.

2.3.3 Overordnede prinsipper for autorisasjon

Prinsipper for å styre autorisasjon kan beskrives i ulike nivåer, med et hovedskille mellom et overordnet nivå og et iverksettingsnivå. En slik inndeling kan betraktes som en parallell til forskjellen mellom et formålsnivå og et regelnivå, som beskrevet ovenfor i kapittel 2.2. Det er en kvalitativ forskjell mellom et overordnet autorisasjonsprinsipp og et autorisasjonsprinsipp på iverksettingsnivå. Nivåene utgjør altså ikke en hierarkisk inndeling, det kan snarere ses som to forskjellige sfærer. Betegnelsen overordnede prinsipper kan likevel være treffende, fordi de formidler en normativ føring for hva som bør oppnås i den autorisasjonen som iverksettes. Det som iverksettes kan på sin side være mer eller mindre gode oppfyllelser av det overordnede prinsippet. Vurderingene i avhandlingens del III gjelder noen autorisasjons-prinsipper på iverksettingsnivået. Her skisseres kort noen trekk ved overordnede prinsipper.

«Need to know» er det overordnede autorisasjonsprinsippet som det oftest er henvist til, både i regulering og i faglig og fagpolitisk litteratur. Dette prinsippet er av og til omtalt med litt andre ordvalg og i andre språkvarianter. Ut fra de historiske eksemplene som er beskrevet i kapittel 2.3.2 ovenfor, ser det ut for at det opprinnelig ble brukt som et autorisasjonsprinsipp på iverksettingsnivået. Meningsinnholdet, slik prinsippet brukes i mange sammenhenger nå, kan imidlertid ikke forstås like skarpt. Bruken av uttrykket «need to know» har endret

[76] Farene for lavere sikkerhet mot omgåelser dreier seg dels om egenskaper ved en del frittstående sikkerhets-produkter, som er slik at de bør være mest mulig uavhengige av egenskaper ved dataene de skal beskytte. Den siden ved problemet forfølges ikke nærmere. En annen side ved dette er at dynamiske kriterier kan gi større åpninger for «selvautorisering», på måter som ikke fanges opp gjennom tilrettelagte kanaler for å godtgjøre informasjonsbehovet. Dette er drøftet noe nærmere i kapittel 8.5.

karakter, det fungerer nå mer som en overordnet normativ føring. For det første henvises det ofte til et «need to know»-prinsipp uten at det fungerer som et supplement til klassifiserings- og klareringssystemer, eller til andre prinsipper på iverksettingsnivået. For det andre har det blitt mer sjelden, bortsett fra i gangsterfilmer, å oppfatte termen «need to know» som et operativt virkemiddel for å splitte opp informasjonstilgangen slik at enkeltaktører skal gjøre sin del av en jobb uten sammenhengskunnskap. Det er mer rimelig nå å oppfatte «need to know» som en løsrevet retningsgiver for regulering og tilgangspolitikk, som ikke har noe selvstendig innhold utover den måten det realiseres på gjennom konkrete valg på iverksettingsnivået.[77]

For å illustrere hvordan «need to know» fungerer som overordnet autorisasjonsprinsipp, kan det være hensiktsmessig å sammenligne det med motstykket «need to protect». Som overordnet prinsipp vil «need to know» innebære en føring om at tilgangen til opplysninger i utgangspunktet skal være stengt, og at det må tildeles positivt uttrykt autorisasjon for de som skal ha tilgang eller handlingsmuligheter. Med «need to protect» som overordnet prinsipp er utgangspunktet motsatt, det innebærer at opplysningene i utgangspunktet er tilgjengelige, og at det må angis konkrete restriksjoner for det som ikke skal være tilgjengelig for alle.[78]

Hvilket overordnede prinsipp som er mest hensiktsmessig, beror på konkrete trekk ved den aktuelle informasjonsbehandlingen. Offentlig publisering, for eksempel av lovtekster eller av generelle kostholdsråd til gravide, har en utpreget «need to protect»-orientering. Det samme gjelder prinsippet om offentlighet i forvaltningen. Utgangspunktet er allmennhetens rett til innsyn, unntakene krever hjemmel.[79] For personopplysninger generelt, og helseopplysninger spesielt, er det imidlertid mer nærliggende å ta utgangspunkt i «need to know»-prinsippets strengere normative føring. Det finnes imidlertid også visse beskjedne elementer av en «need to protect»-orientering på dette området, for eksempel innen pasientstyrt tilgangskontroll.

---

[77] Et autorisasjonsprinsipp på iverksettingsnivå, kalt *the principle of least privilege*, har imidlertid klare fellestrekk med den betydningen «need to know» hadde før det endret karakter til et overordnet prinsipp. Dette prinsippet dreier seg om at en databrukers autorisasjon skal kalkuleres og utformes slik at man får tildelt den minste mengden av handlingsmuligheter som er nødvendig. Jf. Jerome H Saltzer og Michael D Schroeder (1975): «The Protection of Information in Computer Systems». I: *Proceedings of IEEE,* s. 1278–1308.

[78] Denne spesielle bruken av uttrykket «need to protect», som motstykke til «need to know», har en viss utbredelse i fagmiljøer som driver med praktisk informasjonssikkerhetsarbeid. Uttrykket synes å være lite brukt i vitenskapelig litteratur. Det finnes imidlertid enkelte eksempler, blant annet er det brukt i denne betydningen i Roy Campbell m. fl. (2003): «Towards Security and Privacy for Pervasive Computing». I: *Software Security — Theories and Systems*, s. 77–82.

[79] Offentleglova, 19. mai 2006 nr. 16 § 3.

2.3.4 Tildeling av autorisasjoner

I teori om tilgangskontroll er det også inndeling i to hovedstrategier for hvordan autorisasjon kan tildeles. Den ene hovedstrategien kalles obligatorisk tilgangskontroll, som betyr at en databruker får sin autorisasjon fra en instans som har tildelingsfullmakter innen virksomheten. Databrukeren kan da ikke selv beslutte hvilke andre personer som skal få tilgang. Den andre hovedstrategien kalles på norsk enten brukerstyrt eller skjønnsbasert tilgangskontroll. Det innebærer at den som er representert som «eier» av et informasjonselement selv kan beslutte hvilke andre databrukere som skal gis tilgang.[80]

En obligatorisk tilgangskontroll innebærer at det må finnes en besluttet tilgangspolitikk, og besluttede kriterier for hvem som skal få tilgang til hva. Forutsetningen er at behovet for informasjon kan kartlegges a priori. Tilordning er da det samme som å iverksette sentralisert kontroll. Obligatorisk tilgangskontroll gjør det prinsipielt mulig å besvare et spørsmål om hvilke personer som på et gitt tidspunkt kan se, endre eller videreformidle et konkret informasjonselement.

Brukerstyrt tilgangskontroll går ut på at den enkelte databruker selv kan være autorisert for å bestemme over videre tilordning av autorisasjoner. Et område der denne strategien er svært utbredt er i operativsystemers styring av tilgang til kataloger og filer. Operativsystemer bruker ofte termen «eier» om den databruker som har opprettet en fil, og gir denne «eieren» fullmakt til å bestemme hvilke tilganger andre databrukere skal ha.[81] Det innebærer at man også kan tilordne samme tilordningsfullmakt videre til en annen databruker. Riktignok er autorisasjoner i operativsystemer ikke absolutt brukerstyrte, det vil finnes muligheter for sentrale begrensninger og overstyring. Et annet område, der det kanskje kan sies at innslaget av brukerstyring er enda større, er åpne e-postsystemer. For å videreformidle informasjon gjennom åpne kanaler er det normalt tilstrekkelig at man selv har tilgang til informasjonen og kanalen, uten å være representert som eier av, eller ansvarlig for, informasjonen. Ved en rendyrket brukerstyrt tilordning av tilganger finnes det ikke noen reell kontroll med informasjonsflyten. Virksomheten vil ikke kunne besvare et spørsmål om hvem som har sett, eller har kunnet se, et konkret informasjonselement.

---

[80] Disse strategiene kalles i engelskspråklig litteratur henholdsvis *Mandatory Access Control* (med akronymet MAC) og *Discretionary Access Control* (med akronymet DAC). I likhet med «need to know» refererte også begrepene MAC og DAC opprinnelig til mer konkret tilgangspolitikk. Tidlige henvisninger til MAC betegnet ofte dette som den militære modellen, mens DAC ble ansett som mer egnet for kommersielle anvendelser. Over tid har det blitt vanligere å bruke MAC og DAC mer snevert, som ulike teoretiske hovedstrategier for selve tilordningen av autorisasjon. Jf. Vincent C. Hu m. fl. (2006): «Assessment of access control systems», s. 6–7.

[81] Her settes «eier» i anførselstegn, fordi måten dette begrepet brukes på innen teori om tilgangskontroll ikke svarer direkte til et alminnelig eierbegrep. Spørsmålet er nærmere drøftet i kapittel 6.1.3 nedenfor.

Man kan vanskelig gi noe allmenngyldig svar på hva som er mest hensiktsmessig av obligatorisk eller brukerstyrt tilordning. Obligatorisk tilordning er lite fleksibelt, og kan enten føre til mangel på nødvendig informasjon eller til at autorisasjonene defineres uforsvarlig vidt for å unngå slike mangler. Brukestyrt tilordning er mer fleksibelt, men stiller vesentlig større krav til sikkerhetskultur, lojalitet og påpasselighet hos hver databruker.

I mange henseender er de helserettslige reglene, særlig om taushetsplikt og alle unntakene fra taushetsplikten, mer rigide og mindre fleksible enn de personopplysningsrettslige reglene som gir den enkelte virksomhet et relativt stort handlingsrom.[82] Spørsmålet om tilordnings-strategi kompliserer dette bildet av hvor man finner størst grad av henholdsvis rigiditet og fleksibilitet. Selv om valg av tilordningsstrategi ikke er direkte regulert, verken i helseretten eller i personopplysningsretten, følger det av den generelle systematikken at store deler av ansvaret for å oppfylle helserettslige reguleringer gjelder helsepersonell som individer. Reguleringen av informasjonssikkerhet, som på dette området primært er forankret i person-opplysningsretten, vektlegger i større grad virksomhetens ansvar og handlingsrom. Dermed peker den prinsipielt sett mer fleksible informasjonssikkerhetsreguleringen i retning av en strammere strategi for tilordning av autorisasjoner.

[82] Dette belegges i større detalj i kapittel 6.

3 Individuelle og institusjonelle aktører

En begrepsinndeling, med opprinnelse i klassisk, romerrettslig ontologi, skiller mellom handlinger, gjenstander og personer. Avhandlingens tittel gir de viktigste stikkordene for gjenstander og handlinger. I det tredje begrepet ligger det også en viktig nøkkel til å forstå hva problemene med å regulere og kontrollere behandling av helseopplysninger går ut på. Aktørene, avhandlingens «hvem», kan deles inn i følgende hovedkategorier:[83] De som helseopplysningene gjelder, altså pasientene, individuelt helsepersonell, virksomheter som behandler helseopplysninger, og en mer uensartet kategori av de som legger premisser uten selv å behandle helseopplysninger. I drøfting av konkrete regler og relasjoner er det behov for både å detaljere og å gjøre tilføyelser til disse kategoriene. Dette kapitlets relativt grovmaskede aktørkategorier tydeliggjør imidlertid enkelte grunnleggende sammenhenger og motsetninger, som det kan være vanskeligere å rette oppmerksomhet mot på detaljplanet.[84]

Pasienter, helsepersonell og virksomheter har alle en viss autonomi, eller grunnleggende «seg selv-het». Hver aktørkategori har sitt eget grunnlag for sin autonomi, som kommer til syne i merkelappene pasientautonomi, profesjonsautonomi og institusjonell autonomi. Et fellestrekk på tvers av grunnlagene for autonomi er at man forutsetter å kunne bestemme over seg selv i betydelig grad, samtidig som man opptrer ansvarlig og respekterer andre hensyn enn rene egeninteresser. Ingen av aktørenes autonomi er absolutt, det finnes ulike rettslige, strukturelle og kulturelle betingelser som både styrker og svekker en aktørs autonomi. I relasjonene mellom aktørkategorier kan det være både sammenfall og konkurranse mellom én aktørs autonomi og en annen aktørs autonomi, plikter, oppgaver eller verdensbilde.

[83] I juridisk sammenheng er ikke en så generell term som aktør vanlig. Det velges oftere begreper som skiller mellom parter, eller eventuelle andre som involvert i et saksforhold, og det prosessuelle apparatet som befinner seg på utsiden av saksforholdet og bidrar på ulike vis til at rettsspørsmålene får sin løsning. Her går imidlertid analysestrategien ut på å betrakte alle aktørkategoriene som involverte, mens forskeren står utenfor. Det finnes også eksempler på et helt generelt aktørbegrep i juridisk sammenheng: Vold eller trusler (med videre) mot en aktør i rettsvesenet er straffbart, og da med en vid definisjon av «aktør» som omfatter begge sider av skillet mellom innenfor og utenfor saksforholdet, jf. straffeloven [1902], 22. mai 1902 nr. 10 § 132a (2).

[84] I en del sosiologisk teori er «aktør» et temmelig meningsmettet begrep. Dette kapitlet bygger ikke systematisk på en bestemt teori om aktører, men låner inn enkelte teoretiske perspektiver som kan belyse noen egenskaper ved disse aktørkategoriene, og i relasjonene mellom dem.

3.1 Pasienten, og pasientens nærstående

To legaldefinerte begreper, henholdsvis «pasient» og «registrert», utgjør grunnlaget for hvem som hører inn under denne aktørkategorien.[85] Pasienten er i denne sammenheng den person helseopplysningene dreier seg om, enten det gjelder et nåtidig, fremtidig eller avsluttet pasientforhold. I en del sammenhenger, også i helsesektorens fagpolitiske dokumenter, er det vanlig å omtale den som en virksomhet eller tjeneste er til for med det mer nøytrale ordet «bruker». Å betegne pasienten som bruker understreker at det å være pasient ikke beror direkte på hvor syk man er.[86] I avhandlingen her er det imidlertid ingen særskilt grunn til å etterstrebe den nøytrale valøren som begrepet «bruker» kan tilby, og de nevnte definisjonene innebærer ingen reelle innsnevringer.

Krav til eller forutsetninger om samtykke er ofte betraktet som det klareste rettslige uttrykket for pasientautonomi, og da er det vanlig å se pasientautonomi som motsatsen til en paternalistisk helsetjeneste.[87] Paternalismens minst sjarmerende trekk er at det tas for gitt at legen, øvrig helsepersonell, eller «systemet» vet best på vegne av pasienten. Det har nærmest blitt litt vanskelig å bruke ordet paternalisme i en balansert drøfting, fordi det gjerne er fremstilt som del av en evolusjonsfortelling om tidligere uvaner som nå er avløst av en både i medisinsk og etisk forstand bedre pasientautonomi. Som de fleste slike fortellinger er den i hovedsak riktig, men ikke tilstrekkelig nyansert for alle formål.

Et uttrykk som brukes i en del sammenhenger, og som er mindre belastet med negative konnotasjoner enn paternalisme, er standarden «pasientens beste».[88] Utgangspunktet er fortsatt profesjoner som vet best på vegne av pasienten, men i tillegg til en faglig forsvarbar vurdering av hva som er best forutsettes også lydhørhet og evne til å balansere interesser.[89] I

---

[85] Definisjonene lyder «pasient: person som henvender seg til helsetjenesten med anmodning om helsehjelp, eller som helsetjenesten gir eller tilbyr helsehjelp i det enkelte tilfelle», pasientrettighetsloven, 2. juli 1999 nr. 63 § 1-3(1) og «registrert: den som helseopplysninger kan knyttes til», helseregisterloven § 2(1)(10).

[86] Dette følger for så vidt av den norske legaldefinisjonen, men poenget er kanskje enda tydeligere i definisjonen i «Amsterdamerklæringen», *A Declaration on the Promotion of Patients' Rights in Europe.* (1994), s. 15: «Patient(s): User(s) of health care services, whether healthy or sick.»

[87] Se for eksempel Reidar Pedersen m. fl. (2007a): «Pasientautonomi og informert samtykke i klinisk arbeid». I: *Tidsskrift for Den norske legeforening,* s. 1644–1647.

[88] Likevel er «pasientens beste» en standard som signaliserer et visst avhengighetsforhold til profesjonen. Tilsvarende vil gjelde andre standarder som følger samme formel, men som er rettet mot andre klientrelasjoner, for eksempel «barnets beste», som blant annet er brukt i FNs barnekonvensjon. Med en fellesbetegnelse kan dette kalles beste interesser-standarder, lånt fra den tilsvarende engelske betegnelsen *best interests standards*.

[89] Følgende er et eksempel på en forklaring av standarden *pasientens beste,* som legger betydelig vekt på balanseringen mot andre hensyn: «Leger har lange tradisjoner for å vurdere hva som er til pasientens beste og kombinere faglig objektivitet med engasjement for pasienten. … Det kan imidlertid være utfordrende å skape rom for reell dialog og beslutninger som er tilpasset pasientens preferanser og verdier. Leger kan være handlings- og faktaorienterte og være underlagt effektivitetskrav, noe som kan gi mindre plass for de vanskelige

beste interesser-standarder er autonomien likevel underordnet den faglige vurderingen, og i mange tilfeller vil det ha svært gode grunner for seg.[90]

Bruk av helseopplysninger, i helsetjenesten og ellers i samfunnet, er ikke avgrenset til pasientens behov for helsehjelp.[91] Derfor har spørsmål om pasientautonomi større rekkevidde enn bare å handle om graden av selvbestemmelse i de konkrete behandlingssituasjonene. Motsatsen til pasientautonomi er ikke bare den paternalistiske profesjonsutøver. Det dreier seg også om muligheten for selv å kunne trekke grensene for hvor langt pasientrelasjonen som sådan skal rekke. Når helseopplysningene forlater den behandleren pasienten selv har oppsøkt, blir autonomiens motsats en system- og institusjonsverden som kan utydeliggjøre grensene mellom ellers atskilte sfærer i pasientens liv.[92] Videreformidling av helseopplysninger, mot pasientens ønske eller uten pasientens vitende, er i enkelte sammenhenger berettiget. Det innebærer imidlertid like fullt en svekket autonomi: Pasienten får mindre kontroll over sin digitale representasjons tilstander, handlingsvalg og historie.

Nært knyttet til aktørkategorien pasient finnes det ofte enkeltpersoner i pasientens private sfære som har betydning for håndteringen av helseopplysninger. De vanligste betegnelsene er pårørende, eller nærstående personer.[93] Forholdet mellom pasient og nærstående er ikke nødvendigvis ukomplisert, det er lett å se for seg situasjoner der pasienten er vel så bekymret for at visse helseopplysninger tilflyter nærstående som for at fagpersoner blir kjent med opplysningene uten at det foreligger et tjenestelig behov. I utgangspunktet er både de nærståendes egen tilgang til opplysninger, og deres adgang til å påvirke behandlingen av helseopplysninger, underordnet pasientens egen råderett. De mest omfattende unntakene fra dette utgangspunktet gjelder situasjoner der pasienten selv ikke er i stand til å utøve egen råderett, av praktiske eller formelle årsaker. Unntakenes grunnleggende forutsetning er at den

---

samtalene, tvil, usikkerhet og alternative perspektiver.» Reidar Pedersen m. fl. (2007b): «Behandlingsunnlatelse, etikk og jus». I: *Tidsskrift for Den norske legeforening,* s. 1648–1650. (s. 1649).

[90] Slike situasjoner, der det antas at autonomien må vike for en bredere faglig vurdering av «beste interesser», er edruelig drøftet blant annet i Henriette Sinding Aasen (2008): «Barns rett til selvbestemmelse og medbestemmelse i beslutninger om helsehjelp». I: *Tidsskrift for familierett, arverett og barnevernrettslige spørsmål,* s. 4–27, og i Lars Johan Materstvedt og Aslak Syse (2006): «Døendes rettsstilling». I: *Tidsskrift for Den norske lægeforening,* s. 488–489.

[91] I kapittel 5 beskrives noen trekk ved omfanget av samfunnets bruk av helseopplysninger.

[92] Manglende egen kontroll med grensene mellom ulike livssfærer kan også være en motsats til pasientautonomi i den mer snevre paternalistiske betydningen. Uttrykket «totale institusjoner», brukt om asyler, dreier seg blant annet om det: «A basic social arrangement in modern society is that the individual tends to sleep, play and work in different places, with different co-participants, under different authorities, and without an overall rational plan. The central feature of total institutions can be described as a breakdown of the barriers ordinarily separating these three spheres of life.» Erving Goffman (1961): *Asylums. Essays on the social situation of mental patients and other inmates*, s. 5.

[93] Pårørende er definert i pasientrettighetsloven § 1-3(b). Utgangspunktet er at nærmeste pårørende er den pasienten selv oppgir. Dersom pasienten er ute av stand til å oppgi pårørende, angir legaldefinisjonen et hierarki over hvilke nærstående personer som skal kunne fylle en slik funksjon.

nærmeste pårørende er på pasientens side, vil kunne handle på vegne av pasienten, og kommer til å ta hensyn til pasientens egne interesser.[94] Det kan imidlertid være et stort praktisk problem for enkelte pasienter, både blant de myndige og de avhengige, å regulere hvilken deltakelse eller innblanding man ønsker fra sine nærmeste til en hver tid. For en myndig pasient vil dette prinsipielt sett, men kanskje ikke alltid i praksis, være ivaretatt ved at man selv oppgir hvem som er nærmeste pårørende. Spørsmålene som gjelder kontroll med helseopplysninger mellom pasient og nærstående ligger utenfor denne avhandlingens omfang.

3.2 Individuelt helsepersonell og deres medhjelpere

Autorisasjonsordningen i helsepersonellovens kapittel 9 omfatter 29 grupper helsepersonell.[95] Statens autorisasjonskontor for helsepersonell, underlagt Helsedirektoratet, utsteder autorisasjon eller lisens til hver enkeltperson som skal arbeide innen en av disse kategoriene. For å bli autorisert kreves blant annet dokumentasjon av relevant utdannelse og gjennomført praktisk tjeneste, og at man ikke er uegnet for yrket. Helsetilsynet kan tilbakekalle, suspendere eller begrense en autorisasjon fra en som viser seg å være uegnet på grunn av grove pliktbrudd eller spesielle personlige problemer.[96] En helseinstitusjon, eller en annen arbeidsgiver som ansetter en person, kan verken innvilge eller trekke tilbake vedkommendes autorisasjon som helsepersonell.[97] Betydelige deler av den reguleringen som drøftes her, har form av plikter og rettigheter for individuelt helsepersonell.

Autorisering av enkeltindivider, som derved får inngå i et legalt yrkesmonopol, er et av flere trekk som kan styrke en yrkesgruppes posisjon som profesjon.[98] Selv om statsautoriseringen av helsepersonell har blitt svært omfattende etter at nåværende helsepersonellov trådte i kraft, er det likevel neppe meningsfullt å regne alle de 29 helsepersonellgruppene med individuell autorisering som profesjoner i snever forstand. Etter den tradisjonelle profesjonssosiologien er det antakelig bare legene og tannlegene blant helsepersonellgruppene som kan reg-

[94] At nærmeste pårørende både har rett til informasjon i slike tilfeller, og at de forutsettes å handle i samforstand med pasienten, kommer særlig til uttrykk i pasientrettighetsloven §§ 3-3 og 3-4.
[95] Hver enkelt gruppe er oppført i helsepersonelloven § 48(1)(a–å).
[96] Helsepersonelloven §§ 57–59.
[97] Det er en vesentlig forskjell mellom statsautorisering og autorisering som en av hovedaktivitetene innen tilgangskontroll, jf. kapittel 2.3. I forbindelse med tilgangskontroll er det normalt den utøvende virksomheten som administrerer autorisasjoner, og i avhandlingen brukes ordet autorisering hovedsakelig i den betydningen.
[98] Etter det som kan betegnes som en «klassisk» profesjonssosiologi er de viktigste kjennetegnene på en profesjon, i tillegg til en formell autorisasjon som kan inndras, en klar kobling mellom en bestemt utdanning og yrket, en klientrelasjon der profesjonsutøverne vet best på vegne av klienten, og etiske normer som er gjenstand for en form for organisert profesjonsintern oppfølging, jf. Ulf Torgersen (1972): *Profesjonssosiologi*.

nes som rene profesjoner. Legestanden hadde en klar profesjonsprofil også før statsautoriseringen av leger ble innført med den første legeloven.[99] Før dette ga medisinsk embetseksamen automatisk praksisrett, og man avga et etisk legeløfte i forbindelse med embetseksamen. Allerede i 1891 vedtok legeforeningen yrkesetiske regler, som et første skritt mot en profesjonsintern selvjustis.[100] Flere andre grupper av helsepersonell har senere i større eller mindre grad blitt mer profesjonsorienterte, et eksempel er fremveksten av en forskningsbasert sykepleievitenskap som grunnlag for den utdanningen som er påkrevd for å autoriseres som sykepleier.

Profesjonsperspektivet har mange sider som ikke behandles videre i denne avhandlingen. For eksempel har potensielle eller faktiske maktkamper mellom ulike profesjoner, slik som spørsmålene om hvem som skal kunne ha bestemte lederfunksjoner eller hvem som skal kunne utføre hvilke oppgaver, svært liten betydning i denne sammenhengen. Det spiller heller ikke noen vesentlig rolle hvor nær opp mot en «ren profesjon» den ene eller andre gruppen av autorisert helsepersonell befinner seg, både reguleringen og kontrolltiltakene er relativt upåvirket av det. Helsepersonelloven tillegger alle grupper av helsepersonell grunnleggende profesjonsetiske plikter.[101] Det er imidlertid en forskjell mellom individuelt helsepersonell og andre enkeltindivider, ansatt i virksomheter utenfor helsesektoren, som ikke er helsepersonell eller helsepersonells medhjelpere. Når helseopplysninger videreformidles fra helsesektoren til virksomheter utenfor, slik som politi, velferdsforvaltning, skoler og forsikringsselskaper med videre, vil annen regulering enn den profesjonsbestemte taushetsplikten gjelde.[102]

Den viktigste siden ved profesjonsperspektivet her er relasjonen mellom virksomheten og den enkelte individuelle yrkesutøver. Profesjonsutøverne har, og skal ha, en betydelig faglig autonomi. Statlig autorisering er et konkret uttrykk for en viss uavhengighet av den virksomheten man arbeider i. Virksomheten kan mene at en ansatt som er autorisert helsepersonell har gjort en dårlig jobb, men den kan ikke beslutte at vedkommende er uegnet. Mindre konkret, men likevel mer tungtveiende, er argumentet om at profesjonsutøverens relative uavhengighet av virksomheten er selve grunnlaget for en god pasientrelasjon.

---

[99] Legeloven [1927], 29. april 1927 nr. 1, (Opphevet).

[100] Se Per Haave (2007): «Da legene skulle autoriseres». I: *Tidsskrift for Den norske lægeforening,* s. 3267–3271. Artikkelen dokumenter faglig uenighet om hvorvidt statsautorisering (som alternativ til autorisering fra utdanningsinstitusjonen) ville gå på bekostning av den faglige autonomi eller ikke.

[101] I en klassisk profesjonssosiologisk artikkel er en av de grunnleggende profesjonsetiske normene – uavhengig av hvilken profesjon det gjelder – formulert slik: «Be aware of the limited competence of your own specialty within the profession, honor the claims of other specialties, and be ready to refer clients to a more competent colleague», Harold L. Wilensky (1964): «The Professionalization of Everyone?». I: *The American Journal of Sociology,* s. 137–158. (s. 141). Denne normen er helt i tråd med plikten til å innhente bistand og innrette seg etter egne faglige kvalifikasjoner, som er en del av helsepersonellovens forsvarlighetsnorm, jf. helsepersonelloven § 4(2).

[102] Mer detaljert fremstilling av reguleringen, med referanser, følger i kapittel 6.

Likevel er reguleringen av relasjonen mellom individuelt helsepersonell og virksomheter som behandler helseopplysninger, forsiktig sagt, noe ambivalent. Individuelt helsepersonell er underlagt virksomhetens organisering og kontroll. I tillegg til å være autonom fagperson er han også en brikke i systemet, et redskap for virksomhetens måloppnåelse, og en sikkerhetsrisiko. Byråkratisering og komplekse organisasjoner bidrar til å svekke profesjonsautonomiens kår:

> An increasing percentage of professionals work in complex organizations (scientists, engineers, teachers, architects, even lawyers and physicians). These organizations develop their own controls; bosses, not colleagues, rule—or at minimum, power is split among managers, professional experts, and lay boards of directors. The salaried professional often has neither exclusive nor final responsibility for his work; he must accept the ultimate authority of non-professionals in the assessment of both process and product.[103]

Dette bildet er ikke entydig, profesjonsautonomien vil likevel stå relativt sterkt i virksomheter der store andeler av de ansatte er profesjonsutøvere, og der dette preger arbeidsformen.[104] Det faglige skjønn har betydelig vekt i kravene til forsvarlig helsehjelp, og det knyttes i større grad til individuelt helsepersonell enn til virksomheten.[105]

Den profesjonsorienterte reguleringen som er av størst betydning for tilgang til og videreformidling av helseopplysninger er taushetsplikten, med sine unntaksbestemmelser. Unntakene innebærer i en del sammenhenger en frihet til å videreformidle opplysninger, basert på profesjonsutøverens skjønn. Det finnes imidlertid også enkelte rene plikter, som uten videre er bindende for profesjonsutøveren, til å videreformidle opplysninger.

Kategorien «medhjelper», som er nevnt i dette kapitlets overskrift, brukes om personer som bistår autorisert helsepersonell.[106] Historisk sett har kategorien medhjelper omfattet de fleste i helsetjenesten som ikke er leger,[107] mens det etter dagens regelverk bare vil gjelde de som ikke tilhører en av de mange definerte gruppene helsepersonell. Medhjelperens taushetsplikt er av samme art og omfang som for helsepersonellet. Medhjelperkategorien er imidlertid

---

[103] Wilensky (1964), s. 146.
[104] Wilensky (1964), s. 147. Hvor sterk innflytelse profesjoner har eller bør ha over de systemene der profesjonsutøverne arbeider er et sentralt spørsmål også i nåtidig teori om profesjonsmakt, jf. Rune Slagstad (2009): «Styringsvitenskap – ånden som går». I: *Nytt Norsk Tidsskrift,* s. 411–434. (s. 426–427), og Kristian Andenæs (2006): «Om maktens rettsliggjøring og rettsliggjøringens maktpotensial». I: *Tidsskrift for samfunnsforskning,* s. 587–599. (s. 592–593).
[105] Dette kommer særlig til uttrykk i helsepersonelloven § 4(3): «Ved samarbeid med annet helsepersonell, skal legen og tannlegen ta beslutninger i henholdsvis medisinske og odontologiske spørsmål som gjelder undersøkelse og behandling av den enkelte pasient.»
[106] Helsepersonell har en generell adgang til å la seg bistå av medhjelpere såfremt det er forsvarlig, og medhjelperen er da underlagt helsepersonellets kontroll og tilsyn, jf. helsepersonelloven § 5.
[107] Jf. legeloven [1927] § 14(2): «Samme taushetsplikt har lægens medhjelpere.»

fremdeles relativt vid, den omfatter for eksempel de som bistår med elektronisk bearbeiding av helseopplysninger, herunder også teknisk vedlikehold av utstyr for slik bearbeiding.[108]

3.3 Virksomheter som behandler helseopplysninger

Den aktørkategorien som er viet størst oppmerksomhet i avhandlingen hører inn under samlebetegnelsen virksomheter. Vektleggingen av denne kategorien er en nærmest selvfølgelig konsekvens av tittelens presisering av omfanget, «på tvers av IT-systemer og organisatoriske grenser.»

Det er et høyt antall virksomheter som, undergitt visse vilkår og krav, skal eller kan behandle helseopplysninger om identifiserbare pasienter. Med en litt enkel systematikk kan man dele disse virksomhetene i tre lag. Det innerste, og mest pasient- og profesjonsnære laget, er helsetjenesten.[109] Helsetjenesten omfatter det en pasient kommer i kontakt med i behandlingssammenheng, fra små legekontorer til store sykehus, og ved alle typer somatiske eller psykiatriske behov for helsehjelp.

Det neste laget kan kalles helseforvaltningen, her forstått som virksomheter innen helsesektoren som ikke er helsetjeneste, men som behandler helseopplysninger for andre angitte formål.[110] De viktigste aktørene i denne kategorien er de som administrerer sentrale og regionale helseregistre, for eksempel for administrasjon eller epidemiologisk forskning. Slike registre inneholder ofte aggregerte opplysninger, som behandles for formål som ikke er direkte knyttet til helsehjelpen slik pasienten har erfart den. I enkelte slike registre samles det også inn opplysninger over lange tidsrom, og som dekker flere forskjellige sykdomstilfeller og behandlingsforløp for samme pasient.

Det tredje laget av virksomheter er de som befinner seg utenfor helsetjenesten og helseforvaltningen.[111] Denne kategorien omfatter svært ulike formål og virksomheter. Hovedsakelig dreier det seg om virksomheter innen offentlig forvaltning, som velferdsforvaltning,

---

[108] Jf. helsepersonelloven § 25(2), som også gir denne gruppen samarbeidende personell et selvstendig grunnlag for unntak fra taushetsplikten, «… når slik bistand er nødvendig for å oppfylle lovbestemte krav til dokumentasjon.»

[109] Denne betegnelsen er legaldefinert i pasientrettighetsloven § 1-3(d): «helsetjenesten: primærhelsetjenesten, spesialisthelsetjenesten og tannhelsetjenesten.» Betegnelsen er også knyttet til det at en virksomhet yter helsetjenester, jf. helsetilsynsloven, 30. mars 1984 nr. 15 § 3.

[110] Ordet helseforvaltning er anvendelig her fordi helseregisterlovens angitte virkeområde er «helsetjenesten og helseforvaltningen», jf. helseregisterloven § 3. Dermed er det rimelig å velge betegnelsen «helseforvaltning» om virksomheter som er databehandlingsansvarlige etter helseregisterloven (jf. § 2 nr. 8), uten å være helsetjeneste.

[111] Det er som regel den generelle personopplysningsloven, 14. april 2000 nr. 31, og ikke helseregisterloven, som da kommer til anvendelse.

politi, barnevern eller skole. Det forekommer også at private virksomheter, som for eksempel den registrertes forsikringsselskap eller arbeidsgiver, kan behandle helseopplysninger. I de fleste situasjoner behandles helseopplysningene med den registrertes samtykke, og i tråd med den registrertes interesser, men det finnes også situasjoner der det er anledning til å behandle opplysninger uten samtykke. Avhandlingen omhandler ikke all behandling av helseopplysninger i eller mellom virksomheter i dette ytterste laget. Disse virksomhetene omtales bare i den utstrekning de mottar helseopplysninger som er videreformidlet, med berettigelse, fra en virksomhet innenfor helsetjenesten eller helseforvaltningen.

Når helseopplysninger formidles mellom virksomheter innenfor helsetjenesten og helseforvaltningen, eller fra en slik virksomhet til en aktør utenfor helsesektoren, kan det betegnes som en horisontal utveksling. Ut fra helseregisterlovens systematikk og virkemåte innebærer horisontal utveksling at den virksomhet som mottar opplysninger selv blir databehandlingsansvarlig for sin behandling av opplysningene, med alle de forpliktelser det innebærer. En mottakende virksomhet må selv ha et holdbart grunnlag som berettiger at den behandler opplysningene. Helseopplysninger kan også bevege seg vertikalt mellom virksomheter, i den forstand at en virksomhet setter bort et databehandlingsoppdrag til en annen virksomhet.[112] Selv om kontroll med vertikal samhandling kan være komplisert nok i praksis, er det regulatorisk sett en enklere og mer oversiktlig situasjon enn horisontal utveksling. I denne avhandlingen er det kun horisontal utveksling, mellom autonome databehandlingsansvarlige virksomheter, som er gjenstand for drøfting.

Virksomheter som behandler helseopplysninger har en rekke plikter til å sørge for at helseopplysningene behandles på betryggende måte. Det omfatter blant annet å sikre at virksomheten kan redegjøre for sin berettigelse til å behandle bestemte opplysninger, ivareta og oppfylle den registrertes rettigheter, og hindre urettmessig tilgang til eller bruk av opplysningene. Videre er «sørge for»-plikten også en plikt til å kontrollere at tiltakene for å sikre betryggende behandling faktisk blir iverksatt og fungerer.

I utgangspunktet er den databehandlingsansvarliges handlingsrom svært vidt. Den enkelte virksomhet har prinsipielt stor frihet og fleksibilitet i sin fastlegging av hvordan de vil utøve plikten til å sørge for betryggende behandling.[113] Ved horisontal utveksling av opplysninger øker behovet for å harmonisere både ulike virksomheters standard for hva som skal gjelde

[112] Dette betegnes ofte som «outsourcing». I helseregisterlovens og personopplysningslovens terminologi kalles en virksomhet som utfører oppdrag på vegne av den databehandlingsansvarlige *databehandler*. Databehandleren kan bare behandle opplysninger på den måte som er avtalt med den databehandlingsansvarlige, jf. helseregisterloven § 18.

[113] Omfanget av handlefriheten ligger ikke helt «oppe i dagen». Kapittel 4, om risikobasert internkontroll som reguleringsmetode, utdyper og begrunner denne påstanden.

som betryggende behandling, og metodene for å leve opp til standarden. Dersom den enkelte virksomhet får beholde sitt handlingsrom ubeskåret, vil ingen enkeltinstans ha ansvar for, eller praktisk mulighet til, å innestå for at helseopplysninger som videreformidles blir godt nok sikret hos mottakeren. På den annen side innebærer harmoniserte standarder både svekket autonomi for den enkelte virksomhet, og i en del tilfeller, kanskje særlig i små virksomheter, et mer ressurskrevende og mindre målrettet arbeid med å sikre betryggende behandling.

3.4 Premissgivere som ikke selv behandler helseopplysninger

Aktørkategorien premissgivere brukes her som en fellesbetegnelse for ulike grupperinger som har betydelig reell innflytelse over behandlingen av helseopplysninger, uten at de selv behandler slike opplysninger systematisk eller i nevneverdig omfang. Premissgivere omfatter både formelle og uformelle aktører innen regulering, kontrollvirksomhet, teknologi og kunnskaps- og interessentmiljøer. Premissene er i stor grad rettslig regulering, med lover gitt av Stortinget og forskrifter og annen regulering gitt av departementer og direktorater. Kunnskaps- og interessentmiljøene kan til dels være involvert i den regulatoriske virksomheten, som inviterte bidragsytere, lobbyister eller høringsinstanser. Felles teknologiske omgivelser, samfunns- og sektorinfrastruktur, og teknologistandardisering kan betraktes som en del av de regulatoriske premissene, som forvaltes av aktører innen denne kategorien.[114]

Kontrollvirksomheten ivaretas først og fremst, om man måler i volum og innflytelse, av de statlige tilsynsorganene Helsetilsynet og Datatilsynet. Domstolene og spesielle nemnder, som for eksempel Personvernnemnda og Helsepersonellnemnda, har også hatt stor betydning i enkelte mer avgrensete spørsmål. I tillegg utøver de regionale, etiske forskningskomiteer en betydelig konkret forhåndskontroll med bruk av helseopplysninger i forskningsprosjekter. Kontrollerende aktører kan også både være påvirket av, og selv betraktes som, en del av et kunnskaps- og interessentmiljø.

Videre omfatter kunnskaps- og interessentmiljøene som kan legge premisser for behandling av helseopplysninger pasientorganisasjoner, IT-leverandører, og forskning som er rettet mot helseinformatikk og helsevesenet i systemperspektiv.[115] I tillegg har internasjonale premissgivere betydning for behandling av norske helseopplysninger på flere områder. Et

[114] For eksempel administrerer statsforetaket Norsk Helsenett SF et fysisk nettverk for elektronisk samhandling mellom virksomheter i helsesektoren, der både regelverk og fagpolitiske føringer er integrert i infrastrukturen.
[115] En ydmyk aspirasjon om å inngå blant premissgivere av dette slag finnes også i denne avhandlingen, Herbjørn Andresen (2010): «Tilgang til og videreformidling av helseopplysninger. Regulering og kontroll på tvers av IT-systemer og organisatoriske grenser».

godt og gammelt eksempel er FN-organisasjonen World Health Organization, og deres arbeid med faglige kodeverk.[116] EU har særlig hatt stor innflytelse gjennom personverndirektivet, som ligger til grunn for personopplysningsloven og helseregisterloven. Mer nylig har EU gitt ut et utkast til direktiv om pasientrettigheter, i forbindelse med medisinsk behandling over landegrensene.[117]

I denne avhandlingen er ikke premissgiverne noe hovedtema. De viktigste aktørene er de som behandler opplysningene eller er direkte berørt av dem. Kategorien er hovedsakelig med for å synliggjøre et skille mellom virksomheter som behandler helseopplysninger og andre virksomheter som øver påvirkning. En kanskje enklere inndeling ville være å skille mellom de som regulerer og de som reguleres. Det er likevel to grunner til å bruke den litt løsere betegnelsen premissgiver. Den ene grunnen er at man normalt ikke ville regne kunnskaps- og interessentmiljøer med blant de som regulerer, og dermed miste noe av bredden i holdninger og synspunkter som preger den fagpolitiske debatten om helseopplysninger. Den andre grunnen er at premissgivere som aktørkategori inkluderer interessenter som er pådrivere for teknologiske endringer.[118] Å inkludere teknologipådrivere som aktører kan kanskje bidra til å demme opp for en teknologideterministisk forståelse av endringer i premissene for å behandle helseopplysninger. Selv om man lett kan oppleve den teknologiske utviklingen ikke bare som ønskelig, men også som nødvendig eller uunngåelig, er premissgivernes ulike syn og forkjellige slags engasjement et argument for å betrakte utviklingen som styrbar, og å anse de valg man treffer som viktige. Hele dette området er spekket med meninger, viljer, kunnskaper og tvil. Premissgiverne har stor innflytelse, og de taler – nødvendigvis og heldigvis – ikke med én stemme.

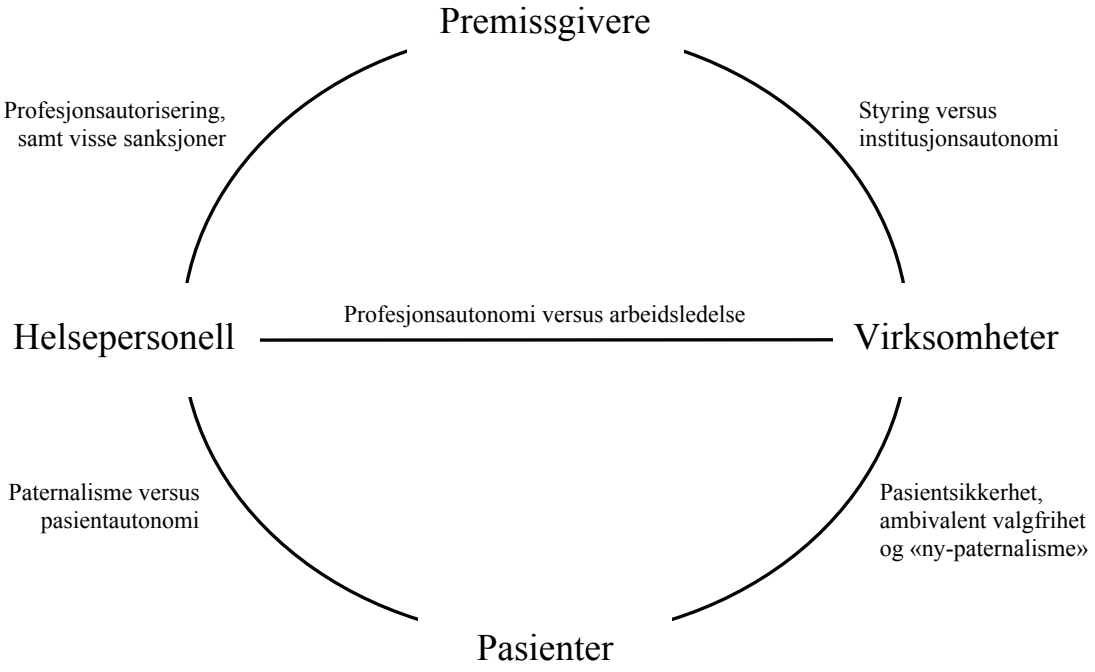
[116] WHO administrerer blant annet kodeverket ICD-10 (International Classification of Diseases, versjon 10). I Norge har ICD-koding vært brukt i en del sammenhenger siden 1951. Versjonsnummeret den gang var ICD-6, som også var den første versjonen av ICD som WHO fikk ansvaret for, jf. World Health Organization: «History of ICD»: *http://www.who.int/classifications/icd/en/*.

[117] KOM(2008) 414. «Forslag til Europa-parlamentets og rådets direktiv om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser»

[118] Et annet, alternativt perspektiv ville være å betrakte teknologien som en premissgivende aktør i seg selv, i tråd med aktørnettverksteori, jf. Bruno Latour (1996): «Social theory and the study of computerized work sites». I: *Information technology and changes in organizational work*, s. 295–307. «Teknologien som aktør»-perspektivet er ikke lagt direkte til grunn her, men kategorien premissgiver åpner for et latoursk perspektiv om *tingene* som det stedet der man håndterer og utøver makt, som er noe av konklusjonen i Marc Berg og Geoffrey Bowker (1997): «The Multiple Bodies of the Medical Record: Towards a Sociology of an Artifact». I: *The Sociological Quarterly,* s. 513–537.

3.5 Relasjoner mellom aktørkategoriene

Ordet autonomi går igjen i presentasjonen av de ulike aktørkategoriene. Det dreier seg likevel om forskjellige egenskaper, autonomien har verken samme begrunnelse eller samme omfang på tvers av disse kategoriene. Autonomi er derfor ikke bare et sammenbindende begrep i aktørinndelingen, det er også en mekanisme for motsetninger og spenningsforhold. Det kan illustreres med en skisse over aktørkategoriene, og noen stikkord som beskriver relasjonene.[119]



Figur 1: Relasjoner mellom aktørkategoriene

Et fellestrekk ved relasjonene mellom aktørkategoriene er at de er dynamiske. Relasjonene utgjør ikke noen fast struktur som er bestemmende for en aktørs handlinger. Det er heller ikke entydige motsetninger mellom én aktørs autonomi og en annen aktørs plikter, rettigheter eller samfunnsoppdrag.[120]

[119] Denne figuren har et visst slektskap med «kvadratmodellen» i Asbjørn Kjønstad (2007): *Helserett: pasienters og helsearbeideres rettsstilling*, s. 31, der et av hjørnene er *staten*, som kan tilsvare den formelle siden av aktørgruppen *premissgivere*. Den viktigste forskjellen mellom min og Kjønstads figur er ikke valg av geometrisk utforming, men hvilke trekk ved relasjonene mellom aktørgrupper som er vektlagt.

[120] Et giddensk perspektiv på aktører vil være ganske dekkende for disse dynamiske relasjonene. Der er aktører et begrep som integrerer strukturer og aktørenes vilje, en aktør bruker strukturen til å legitimere sine handlinger. Strukturene determinerer ikke aktørenes handlinger, men det er heller ikke motsatt: Strukturene er reelle, de dannes og gjenskapes, de eksisterer ikke bare som en observasjon av hvordan aktørene handler. Se Anthony Giddens (1984): *The constitution of society: outline of the theory of structuration*, s. 217–220.

Det er figurens horisontale linje, mellom individuelt helsepersonell og virksomheter, som volder mest besvær i avhandlingens problemstilling. Denne relasjonen, som i forenklet form kan beskrives som en motsetning mellom profesjonsautonomi og ledelse, er i seg selv relativt kompleks. I tillegg påvirkes denne relasjonen på ulike vis av de øvrige relasjonene mellom aktørkategoriene.

I en viss forstand vil det kunne virke kunstig, særlig på bakkeplanet i helsetjenesten, å trekke et skarpt skille mellom profesjoner og virksomhetsnivået. De enkeltpersoner som i kraft av leder- og stabsfunksjoner representerer virksomheten «som system» har svært ofte samme type utdanning og internaliserte normer og verdier som sine underordnede. Helsepersonellet er virksomhetsnivåets kjøtt og blod.[121] Det er heller ikke slik at virksomhetsnivået er mindre helsefaglig forpliktet, mange av de oppgavene som tilligger virksomheten dreier seg om tiltak for å sikre at helsetjenesten er forsvarlig. Reguleringen av henholdsvis helsepersonells og virksomheters oppgaver er imidlertid både komplisert og til dels utydelig. I utgangspunktet er virksomheten ansvarlig for organisering og arbeidsdeling, men det finnes også enkelte oppgaver innen helsetjenesten som har form av legale faglige prerogativer. Visse oppgaver og beslutninger er lagt til individuelt helsepersonell og ikke til virksomheten.[122]

Den profesjonsforankrede faglige styringen er for øvrig ikke bare til stede i den pasient- og profesjonsnære helsetjenesten. Også hos de premissgivende aktørene innen helsesektoren anses den profesjonsforankrede fagstyringen å være solid grunnfestet.[123]

Profesjonsautoriseringen bidrar generelt til å styrke profesjonsutøvernes autonomi overfor den virksomheten der vedkommende er ansatt. Den faglige normen man skal leve opp til er ikke ensidig bestemt av arbeidsgiveren. Når det gjelder behandling av helseopplysninger er det imidlertid en vesentlig forskjell mellom den helserettslige og den personopplysningsrettslige reguleringen. Mens Helsetilsynet kan iverksette visse sanksjoner mot individuelt helsepersonell, kjenner Datatilsynet bare virksomheten. Datatilsynet må forutsette at hver virksomhet øver en tilstrekkelig, men likevel ikke for inngripende, kontroll med sine ansatte.

Det momentet som tradisjonelt kanskje har bidratt med den sterkeste støtten til profesjonsautonomien er den individuelle fortrolighet og tillit mellom pasient og helsepersonell. Selv om pasienten kan ha en begrunnet skepsis til helsepersonell som vet eller mener å vite hva

[121] I større virksomheter vil det riktignok kunne være et betydelig innslag av ansatte med annen bakgrunn, for eksempel teknologer, organisasjonsfaglig personell og jurister, i støttefunksjoner for ledelsen.
[122] Dette er utførlig drøftet i Asbjørn Kjønstad (2005): «Styringsretten i helsevesenet». I: *Arbeidsrett,* s. 1–27. Artikkelen argumenterer for at lovgivningen burde styrke ledelsesansvaret gjennom å avvikle svakt begrunnede «prerogativer» for enkelte grupper helsepersonell.
[123] Jf. vurderingene av det tidligere Helsedirektoratet i Trond Nordby (1993): «Det offentlige helsevesenet – en fagstyrets høyborg». I: *Arbeiderpartiet og planstyret 1945–1964*, s. 105–120.

som er best for ham selv, er likevel helsepersonellet konkrete og fysiske personer. Et argument som forsvarer en individuelt orientert profesjonsautonomi er at profesjonsutøveren kan være pasientens allierte mot et upersonlig og effektivitetsorientert system.[124] Dette argumentet kan blant annet finne støtte i at de mest synlige pådriverne for mer utstrakt videreformidling av helseopplysninger er systemaktører, både premissgivere og virksomheter som behandler helseopplysninger. På den annen side er det individer som gjør feil, bryter regler og overtrer sikkerhetstiltak, enten det skyldes kunnskapsmangel, uaktsomhet eller illojalitet. Virksomhetens evne til å fange opp, korrigere og hindre gjentakelser gir pasienten beskyttelse gjennom å kontrollere de ansatte.[125] Man kan si det har oppstått en ny relasjon mellom virksomhetsnivået og pasienten, der det systematiske arbeidet med kvalitetssikring og kontroll i økende grad ses som grunnlaget for både pasientens og samfunnets tillit.[126] Virksomhetens arbeid for å øke pasientens sikkerhet er prinsipielt sett også en form for paternalisme, med virksomheten som den nye pater. Det samlede bildet, i grove trekk, synes å være en moderat forskyvning i retning av større systemorientering, og noe mindre individuell autonomi for den enkelte profesjonsutøver.

[124] Argumentet er elegant formulert i Tor-Johan Ekeland (2004): «Autonomi og evidensbasert praksis», s. 7: «Skal pasienten t.d. ha tillit til legen sin, må ein oppleve at legen er til for pasienten og ikkje er bunden på hender og føter av andre interesser. Dette er kjernen i den kliniske logikken: klinikaren sin autonomi er ein føresetnad for pasienten sin autonomi.»

[125] En slik utvikling hilses velkommen blant annet av en av pionerene innen vitenskapeliggjøringen av det å behandle helseopplysninger: «The idea of 'my doctor', the all knowing graduate of a credentialed university medical school must be abandoned. In travel, we do not talk about 'my pilot', we talk about the airline system of which the pilot is only one part, and his role is sharply defined and rigorously monitored.» Lawrence L. Weed (2006): «Idols of the Mind» (konferanseartikkel).

[126] Jf. Donald W. Light og Olaf Gjerløw Aasland (2003): «Den nye legerollen – kvalitet, åpenhet og tillit». I: *Tidsskrift for Den norske legeforening,* s. 1870–1873. Denne artikkelen går langt i retning av å karakterisere den individuelle profesjonsautonomien som et slags historisk feilskjær, som til dels har stått i veien for den faglige kvalitetssikringen gjennom systematisk kontroll i et kollektivt profesjonsfellesskap.

4 Risikobasert internkontroll som reguleringsmetode

En vesentlig del av de pliktene en virksomhet har til å utfylle reguleringen av og gjennomføre kontroll med egen behandling av helseopplysninger er utformet som en plikt til å etablere og vedlikeholde et risikobasert internkontrollsystem.[127] Risikobasert internkontroll kan betraktes som en spesiell reguleringsmetode, med visse fellestrekk, men også betydelige forskjeller, på tvers av en rekke samfunnsområder. Som to ytterpunkter kan man enten argumentere for at det er et sterkt metodisk slektskap mellom ulike internkontrollbestemmelser, eller argumentere for at internkontroll er en merkelapp som brukes om en rekke ulike reguleringer uten et slikt slektskap. Dette kapitlet synliggjør både fellestrekk og ulikheter, men bygger på en grunnleggende forutsetning om en stor grad av metodisk slektskap. Kapitlet har to formål: Det ene er å gi belegg for avhandlingens påstand om virksomhetenes aktivitetsplikt og handlingsrom som en viktig side ved den reguleringen som har betydning for informasjonssikkerhet generelt og tilgangskontroll spesielt. Det andre formålet er å drøfte, mer prinsipielt, reguleringsmetodens styrker og svakheter ved horisontal samhandling mellom virksomheter.

En plikt til å etablere internkontrollsystemer har i løpet av de siste tre tiår blitt innført i et høyt antall lover og forskrifter. Plikten er ofte utformet som en forskriftshjemmel.[128] I tillegg finnes det formelle lover som ikke bruker ordene internkontroll eller internkontrollsystemer, men hvor det likevel går klart frem av forarbeider, forskrifter eller innretningen av det statlige tilsynet med virksomheten at det er dette som menes.[129]

De mange pliktene til å etablere internkontrollsystemer har en rekke fellestrekk. Det overordnede fellestrekket – som foreløpig må betraktes som en påstand, som skal belegges

[127] For helseopplysninger følger dette i hovedsak av helseregisterloven §§ 16 og 17 innen helsetjenesten og helseforvaltningen, og ellers av personopplysningsloven §§ 13 og 14.
[128] Et typisk, og tilfeldig valgt eksempel blant mange mulige, er dette: «Kongen kan gi nærmere forskrifter om internkontroll og internkontrollsystemer for å sikre at krav fastsatt i eller i medhold av denne loven overholdes», strålevernloven, 12. mai 2000 nr. 36 § 11. Lignende formuleringer finnes også i en rekke andre lover.
[129] To eksempler på dette er arbeidsmiljøloven [2005], 17. juni 2005 nr. 62 og skipssikkerhetsloven, 16. februar 2007 nr. 9. I begge disse tilfellene er innholdet i bestemmelsene om internkontroll videreført fra deres forløpere i lovsamlingen, men uten at ordet internkontroll nevnes i de nyere lovene.

systematisk gjennom dette kapitlet – er at risikobasert internkontroll som reguleringsmetode står i en atskillig bredere teoretisk og ideologisk sammenheng enn en prima facie forståelse av pliktbestemmelsene i lover og forskrifter tilsier. I dette kapitlet analyseres internkontroll-systemet som en idealtype. Det er en metode som innebærer visse muligheter og begrens-ninger for analysen. Idealtypen er ikke en oppregning av hvilke egenskaper som forekommer hyppigst eller ligger nærmest et «gjennomsnitt» av noen utvalgte internkontrollplikter, det er en konstruert samling egenskaper som tydeliggjør en antatt kjerne i reguleringsmetoden.

En idealtype er en begrepsmessig rendyrkning, som fremhever karakteristiske trekk ved et fenomen i samfunnet. Ordet ideal sikter ikke nødvendigvis til en normativ ønsketilstand, men betegner en tankemessig rendyrking av de typiske trekkene. Idealtypen er en abstraksjon eller generalisering for et analytisk formål.[130] I nyere sosiologisk metodelitteratur er en rekke forutsetninger, muligheter og begrensninger ved idealtypeanalyser drøftet.[131] En av forutset-ningene, som har en viss betydning her, er at ideer eller mening kan være en årsaksfaktor. Mening er en dimensjon ved kulturelle fenomener, for eksempel i form av tanker, motiver, moral, kunnskap, eller oppfatninger om en normativ status – som at noen eier en gjenstand eller at en bestemt handling er forbudt.[132] En annen forutsetning er at de empiriske feno-menene som man undersøker og sammenligner med idealtypen ofte i seg selv er komplekse og vage fenomener som må beskrives gjennom mer eller mindre typiske eksempler, generali-seringer og abstraksjoner. Denne forutsetningen er litt «brysom», fordi den kan bidra til å gjøre det vanskelig å holde klart fra hverandre hva som er beskrivelse av idealtypen og hva som er en fremstilling av de fenomenene som subsumeres under idealtypen.[133] Analysen består dermed ikke av sammenligninger mellom modellen og kjensgjerningene, men mellom

[130] Dette er en utbredt undersøkelsesmetode innen samfunnsvitenskap, og forbindes særlig med sosiologen Max Weber. Et av Webers egne metodeessay beskriver idealtyper slik: «An ideal type is formed by the one-sided *accentuation* of one or more points of view and by the synthesis of a great many diffuse, discrete, more or less present and occasionally absent *concrete individual* phenomena, which are arranged according to those one-sidedly emphasized viewpoints into a unified *analytical* construct (*Gedankenbild*). In its conceptual purity, this mental construct (*Gedankenbild*) cannot be found empirically anywhere in reality. It is *utopia*. Historical research faces the task of determining in each individual case, the extent to which this ideal construct approximates to or diverges from reality.» Max Weber (1994): «Objectivity and understanding in economics». I: *The philosophy of economics: An anthology*, s. 69–82. (s. 81). originale uthevinger.

[131] Tore Lindbekk (1992): «The Weberian Ideal-type: Development and Continuities». I: *Acta Sociologica,* s. 285–297.

[132] Et eksempel Lindbekk gir er Webers kjente idealtype *protestantisk etikk*, der religiøs doktrine om predestina-sjon, kombinert med et psykologisk behov for tegn på at man var blant de frelste, bidro både til å endre menneskers handlinger og til å fremme den moderne kapitalismen. «Meanings thus have two types of effect: they restrain and direct the development of other meanings, and they restrain and direct *action.*» Lindbekk (1992), s. 289, original utheving.

[133] Lindbekk uttrykker det slik: «However, both the ideal-type and the observed, empirical phenomena to which the type is compared are *pictures.* Both of them are abstracted from 'reality' and pretend to represent reality.» Lindbekk (1992), s. 290, original utheving.

to modellnivåer. Formålet med, og resultatene av, en idealtypeanalyse er kvalitative beskrivelser av komplekse fenomener i samfunnet. Mengden av variabler er stor, og prinsipielt åpen.

Selv om idealtyper er tydeligst beskrevet i samfunnsvitenskapelig metodelitteratur, er tilsvarende konstruksjoner ikke ukjente i andre fag. Det kan for eksempel sammenlignes med situasjoner der rettsvitenskapelig litteratur først presenterer en generalisert syntese av tidligere teori og avgjørelser på et område, for deretter å drøfte denne mot nye funn og vurderinger.

4.1 Det idealtypiske internkontrollsystem

Det idealtypiske pliktsubjektet for internkontroll er en virksomhet, som fyller visse kriterier. Kriteriene kan være at virksomheten generelt er omfattet av den aktuelle loven, for eksempel i egenskap av å være arbeidsgiver, eller fordi virksomheten behandler personopplysninger. Andre typer kriterier kan være konkret angitte vilkår, for eksempel at virksomheten driver autorisasjonspliktig næringsmiddelvirksomhet. Plikten vil ofte gjelde likt for offentlige og private virksomheter. Det er som regel virksomhetens art og behovet for å ivareta et angitt samfunnshensyn som definerer denne typen plikter, og ikke eierskap eller selskapsform. Riktignok vil det i praksis være slik at noen arter virksomhet kun drives av private aktører, mens andre kun bedrives av offentlige organer. Det har likevel liten betydning for hva plikten til internkontroll vil innebære. Blant internkontrollbestemmelsene som har størst nedslagsfelt målt i antall omfattede virksomheter, for eksempel kontroll med behandling av personopplysninger eller kontroll med arbeidstakeres helse, miljø og sikkerhet,[134] tolkes og praktiseres internkontroll likt uavhengig av om pliktsubjektet er en offentlig eller en privat virksomhet.

Internkontroll er en metode for å sikre at virksomheter ivaretar et angitt samfunnshensyn godt nok. Samfunnshensynet skal ivaretas innenfor akseptabel risiko. Et samfunnshensyn, det kan kanskje alternativt kalles en offentlig interesse, er i denne sammenheng det overordnede målet som en bestemt plikt til internkontroll skal ivareta. En fellesnevner for de samfunnshensynene som skal ivaretas gjennom internkontroll er at de ikke er, eller oppleves som, virksomhetens egentlige formål eller oppdrag. Samfunnet kan derfor ikke regne det som sikkert at en virksomhet vil ivareta samfunnshensynet av ren egeninteresse, selv om samfunnet og virksomhetene selvfølgelig også gjerne kan ha sammenfallende interesser.

Prinsipielt sett befinner samfunnshensynet seg utenfor idealtypen. Reguleringsmetodens hovedspørsmål er ikke hva som skal ivaretas, men hvorfor og hvordan. Idealtypen internkon-

[134] Alminnelig forkortelse er HMS.

troll, slik den er konstruert her, har tre overordnede aspekter. Det første aspektet er hvorfor-spørsmålene. Stikkordene for å besvare dem er kontinuitet, fleksibilitet og samfunnskontroll. Behovet for kontinuitet henger sammen med at også legitim og ønsket virksomhet i samfunnet kan utgjøre en trussel mot ett eller flere viktige samfunnshensyn. I de aller fleste tilfeller skal virksomheter fortsette til tross for feil eller uforutsette negative hendelser. I forlengelsen av behovet for kontinuitet ligger også en forventning om kontinuerlige forbedringer i virksomhetens arbeid med å ivareta samfunnshensynet. Fleksibilitet er et sammensatt behov, som omfatter forskjeller i skadepotensial, i virksomheters kapasitet for oppfølging og kontroll, og i avveininger mellom ulike samfunnshensyn. Samfunnskontrollen med internkontrollsystemer ivaretas i hovedsak av eksterne tilsynsorganer med et relativt smalt faglig mandat.

For den enkelte virksomhet legger den eksterne samfunnskontrollen også viktige føringer for hvordan-spørsmålene, ved at det stilles krav til dokumentasjon som sikrer at systemet er etterprøvbart for statlige tilsynsorganer, sertifiseringsorganer eller revisorer.

Hvordan-spørsmålene, det som utgjør metodens struktur og prosesser, er det andre og det mest omfattende aspektet ved idealtypen. Motoren i risikobasert internkontroll som reguleringsmetode er aktivitetsplikter som virksomheten skal rette seg etter. Et tilsynsorgan vil ikke kunne akseptere unnlatelser der en virksomhet «stoler på flaksen» som et holdbart tiltak for å ivareta samfunnshensynet. Aktivitetspliktene kan til dels sies å inneholde en ideologisk komponent, i den forstand at en virksomhet skal internalisere samfunnshensynet og bevise etterlevelse. Det er imidlertid pliktene til å utføre en serie med innbyrdes sammenhengende metodetrinn som er idealtypens mest karakteristiske egenskap. Ingen av de enkelte metodetrinnene er nyskapninger som kom inn i norsk rett sammen med plikter til internkontroll. De er heller ikke eksklusivt knyttet til det idealtypiske internkontrollsystem, men finnes igjen i plikter, krav og forventninger på mange ulike områder. Det er den strukturelle sammenstillingen av de idealtypiske metodetrinnene som fører til at en rekke ulike samfunnshensyn, i hvert fall tilsynelatende, reguleres på en mer ensartet måte gjennom risikobasert internkontroll enn de gjorde tidligere.

Det første metodetrinnet er å organisere virksomhetens internkontrollarbeid, og å dokumentere dette arbeidets plass i organisasjonen. Det andre metodetrinnet er å beslutte mål og kriterier for aksept av risiko. I regeltekster og veiledninger om internkontroll er dette ofte beskrevet som to separate aktiviteter. Her er det slått sammen til ett metodetrinn, fordi det strengt tatt er to sider av samme sak. Verbet «å beslutte» er det viktigste elementet i dette metodetrinnet. Målene er en positivt angitt operasjonalisering av hva det innebærer å ivareta samfunnshensynet i den aktuelle virksomheten, mens kriterier for aksept av risiko er virksom-

hetens besluttede feiltoleranse, en negativ angivelse av det samme. Tredje metodetrinn er å gjennomføre risikovurderinger. Det innebærer at virksomheten definerer hva slags hendelser, handlinger og sideeffekter som skal eller bør unngås, og vurderer sannsynligheten for og konsekvensene av dem. Kartlagt risiko sammenlignes med akseptkriteriene. I den grad risikoen overstiger besluttet akseptnivå, gjelder fjerde metodetrinn som er å velge ut og iverksette egnede risikoreduserende tiltak. Femte metodetrinn er å utøve egen kontroll med at de iverksatte risikoreduserende tiltakene fungerer etter hensikten. Det sjette metodetrinnet er avvikshåndtering. Avvikshåndteringen er ikke begrenset til bare å omfatte de situasjonene der et forhåndsdefinert risikoreduserende tiltak har sviktet. Også de negative konsekvensene som man har valgt å akseptere, for eksempel fordi sannsynligheten har vært vurdert som lav nok til at det er forsvarlig, skal fanges opp som avvik.

Det tredje aspektet ved idealtypen er noen mer abstrakte egenskaper ved risikobasert internkontroll som sådan. Disse egenskapene hører ikke inn under metodens hvorfor- og hvordanspørsmål, de kan snarere betraktes som ideologiske, politiske og rettspolitiske momenter til vurderinger av reguleringsmetodens effekter, ønskelighet og egnethet. Årsaken til at dette aspektet er løftet inn i idealtypen, i stedet for å behandles som et selvstendig analysetema, er at de grunnleggende spørsmålene om hvor stort handlingsrom virksomhetene skal ha, balansen mellom faglige og politiske elementer i samfunnskontrollen, og hvilke sider ved samfunnshensynet som kan falle utenfor denne formen for selvregulering, kan ha innvirkning på utformingen og tolkningen av de konkrete internkontrollpliktene.

Det idealtypiske internkontrollsystem er en reguleringsmetode som tilkjenner den enkelte virksomhet et stort handlingsrom. En virksomhet står relativt fritt, både til å beslutte hvordan samfunnshensynet skal avveies mot andre hensyn, og til å velge hvilke tiltak de vil iverksette for å ivareta det. Virksomheten har tilnærmet full suverenitet. Dette aspektet ved idealtypen er også uttrykt som et hypotetisk ytterpunkt i en tidlig, rettsvitenskapelig artikkel om myndighetenes kontroll med sikkerheten i petroleumsvirksomheten:

> Den prosess for å minske risikoen i petroleumsvirksomheten vi her har skissert, kan tenkes overlatt helt ut til virksomhetsutøverne selv. Det ville da være opp til dem å identifisere risikofaktorer og alternative avhjelpninger, definere et akseptabelt risikonivå, velge utformning av utstyr og prosedyrer, og sikre at forutsetningene for valget blir etterlevet. På alle disse punktene ville virksomhetsutøvernes egen vurdering av nytte (i vid forstand) være retningsgivende.[135]

[135] Knut Kaasen (1981): «Norske myndigheters kontroll med sikkerheten i petroleumsvirksomheten på norsk kontinentalsokkel». I: *Tidsskrift for Rettsvitenskap,* s. 82–103. (s. 84).

Både den artikkelen som sitatet er hentet fra, og en rekke rettskilder som definerer eller utdyper konkrete plikter til internkontroll, viser at det finnes mange små og store variasjoner fra dette idealtypiske ytterpunktet i eksisterende reguleringer. Ettersom alle konkrete internkontrollplikter avviker fra idealtypen i større eller mindre grad – det er en direkte konsekvens av å bruke en slik undersøkelsesmetode – kan det være på sin plass med en begrunnelse for at full suverenitet for virksomheten er valgt som idealtypisk utgangspunkt for denne analysen. Det er tenkelig at en annen og mer moderat modellbeskrivelse kunne ha vært mer representativ for eksisterende regler om risikobasert internkontroll. Den suverene virksomhet er valgt som utgangspunkt både fordi det er et slags ytterpunkt som gjør forskjeller fra andre reguleringsmetoder godt synlige, og fordi det legger idealtypen relativt nær opp til de formene for regler om informasjonssikkerhet som har størst betydning for hvordan virksomheter som behandler helseopplysninger kan og bør innrette sin tilgangskontroll.[136]

4.1.1 Rettslig regulering i møte med administrativ og faglig kunnskap

Internkontrollsystemer trenger ikke være det eneste rettslige instrumentet for å ivareta et gitt samfunnshensyn. Andre virkemidler, som forhåndstillatelse til og vilkår for å drive en type virksomhet, detaljerte regler, eller plikt til uavhengig revisjon, eksisterer gjerne side om side med plikten til internkontroll. Minst like viktig er det at internkontroll langt fra er noe rendyrket rettslig instrument. Som de idealtypiske metodetrinnene antyder, dreier det seg om ulike gjøremål som ofte forutsetter en bestemt faglig bakgrunn. Avhengig av hva samfunnshensynet er, kan den faglige bakgrunnen eksempelvis være innen regnskap, miljøvernteknologi, helsehjelp eller informasjonssikkerhet, blant mange andre.

Samtidig innebærer internkontroll også en del oppgaver som er uavhengige av den faglige bakgrunnen. Å arbeide med styringsverktøy som risikohåndtering og kvalitetssikring har i seg selv blitt profesjonaliserte disipliner. Det kan oppstå motsetninger mellom fagkunnskap og den administrative kunnskapen om hvordan man utvikler og opprettholder et internkontrollsystem. Om en virksomhet organiserer internkontroll som en rendyrket administrativ disiplin, på siden av det faglige, er det fare for at viktige tiltak for å ivareta samfunnshensynet aldri blir underlagt systemet. Om man overser den administrative kunnskapen, og lar internkontroll kun være et faglig anliggende, er det fare for at internkontrollsystemet ikke oppnår den kvaliteten

[136] Jf. helseregisterloven § 16 og personopplysningsforskriften kapittel 2 (særlig §§ 2-3, 2-4, 2-8, 2-11 og 2-14), samt den tekniske standarden NS-ISO/IEC-17799:2005.

som skal til for å overbevise tilsynsorganer og samfunnet for øvrig om at systemet fungerer etter hensikten. Idealet er et godt samspill mellom administrativ og faglig kunnskap.

Spenningsforholdet mellom administrativ og faglig kunnskap er til dels forsøkt løst gjennom måten de rettslige pliktene er utformet på. Blant annet har virksomhetene ofte en plikt til å involvere arbeidstakere, begrunnet med at formålet er å utnytte de samlete kunnskapene. I mange tilfeller er motstykket til denne plikten ikke formulert som en rettighet for arbeidstakerne, men som deres plikt til å medvirke. På den annen side kan det også tenkes at lovgivning om internkontroll i seg selv bidrar til å forsterke motsetningene. Et gjennomarbeidet og godt sammensatt internkontrollsystem kan, internt i virksomheten, bli oppfattet som noe som «bare er laget for å innfri myndighetskrav», slik at den rettslig pålagte plikten blir stående i veien for godt samspill mellom fag og administrasjon.

4.1.2 Behovet for fleksible regler

Det idealtypiske utgangspunkt, en høy grad av suverenitet for virksomhetene, må innebære at reglene har en tilsvarende høy grad av fleksibilitet.[137] Sammenhengen mellom de idealtypiske metodetrinnene betinger i seg selv et stort handlingsrom. Dersom det skal være meningsfullt og forsvarlig at en virksomhet selv tar stilling til hva som er akseptabel risiko, så å si på vegne av samfunnet, må også virksomheten stå relativt fritt til å velge hvilke avhjelpende tiltak som egner seg for å oppnå dette.

Behovet for fleksibilitet var fremme i tidlig argumentasjon for å innføre internkontroll i sikkerhetsarbeid, i form av anbefalinger om en endring av sikkerhetskrav fra å anvise fremgangsmåter til å angi funksjonskrav.[138] Det kan diskuteres om funksjonskrav er kvalitativt forskjellig fra krav til fremgangsmåter, eller om det er ulike trinn på en skala av detaljering. Det er imidlertid en diskusjon som ikke egentlig rokker ved at funksjonskrav innebærer større

[137] Da internkontroll som pålegg i lov var nytt i Norge, og fremdeles bare omfattet relativt få virksomheter, ble det fleksible fremhevet som en viktig nyhet: «Min tese er at vi her står over for en ny måte å organisere offentlig kontrollmyndighet på, og en ny måte å lage rettsregler på.» Hans Petter Graver (1984a): «Fleksibilitet som reguleringsteknikk - mot en anarkistisk rettsform». I: *Retfærd. Nordisk Juridisk Tidsskrift,* s. 59–68. (s. 59).

[138] Denne anbefalingen er formulert slik i stortingsmeldingen som gjennomgikk den ukontrollerte utblåsningen på Bravoplattformen i 1977: «Det er en vesentlig oppgave for kontrollmyndighetene å utarbeide mer presise krav til selskapenes virksomhet for at denne skal utøves på en sikkerhetsmessig forsvarlig måte. Dette bør imidlertid etter departementets vurdering ikke alene gjøres i form av detaljerte krav til hvordan denne virksomhet konkret skal utføres. Snarere bør myndighetene søke å definere hvordan virksomheten skal funksjonere. Det vil med andre ord oftest være mer hensiktsmessig å spesifisere hvilket resultat myndighetene vil oppnå, enn å gi anvisning på hvordan dette skal oppnås. … Innen de gitte rammene står rettighetshaverne fritt i å bestemme framgangsmåten for hvordan de vil oppfylle disse kravene. Dermed oppnår en et fleksibelt system som gir rom for nødvendige tilpasninger dersom uforutsette forhold skulle inntreffe under arbeidet. Det vil også gi mulighet for at operatørene i tilstrekkelig grad kan gjøre nytte av den raske og kontinuerlige teknologiske nyvinning som skjer innen denne virksomhet.» Stortingsmelding nr. 65 (1977-78), s. 12.

fleksibilitet for virksomheten.[139] Funksjonskrav innebærer kanskje først og fremst en endring i måten eksterne tilsynsorganer utøver sin kontroll på.[140]

I de mange bestemmelsene om internkontroll som etter hvert har kommet inn i lover og forskrifter, er det ulike måter å markere fleksibilitet i regelverket på. Internkontrollbestemmelsene har neppe egentlig bidratt til å utvide repertoaret av slike markører. Fleksible måter å uttrykke regler på finner man nær sagt over alt. De viktigste forskjellene ligger dels i at internkontrollsystemer har bygget inn flere lag av fleksibilitet gjennom de innbyrdes avhengige metodetrinnene, og dels i aktivitetsplikten. Idealtypen internkontroll innebærer å operasjonalisere og dokumentere hvordan virksomheten velger å forstå og praktisere reglene.

En utbredt måte formelle lover angir krav til internkontrollsystemer på, er å peke tilbake på hjemmelslovens øvrige regler. Internkontrollens angitte formål er da å sikre at kravene i lov eller i medhold av lov oppfylles.[141] Formuleringen «krav fastsatt i eller i medhold av denne lov» tilsier at internkontrollsystemet også må reflektere relevante endringer i loven. Denne utformingen av plikten pålegger virksomhetene å gjennomføre de aktiviteter som er nødvendig for å opprettholde samsvar med til en hver tid gjeldende regelverk.

En alternativ markør er å knytte internkontrollplikten til et angitt samfunnshensyn i form av en rettslig standard. Det vil si en målestokk som har sitt feste utenfor det rettslige, og som kan endre seg over tid.[142] Et eksempel på et samfunnshensyn angitt som en rettslig standard er uttrykket «tilfredsstillende informasjonssikkerhet» som brukes i nesten likelydende bestemmelser i personopplysningsloven og i helseregisterloven.[143] Virksomhetsledelsen, om det er i et sykehus, et lite medisinsk laboratorium eller et helseforskningsinstitutt, må ta stilling til hva som er tilfredsstillende informasjonssikkerhet i egen virksomhet. Anvendelsen av målestokken kan avhenge hva slags opplysninger som behandles, hvordan og hvor lenge de lagres, hvordan og til hvem de kommuniseres, hvor attraktive opplysningene er for en ekstern angriper eller intern utro tjener, med mer. I utgangspunktet er dette faglige vurderinger, men

[139] Et eksempel på at overgangen fra detaljerte krav til funksjonskrav ikke *i seg selv* har vært ansett som en vesentlig endret reguleringsteknikk, finner man i betraktningen om dette som ren «ordmagi», fordi det egentlig bare er et valg mellom ulike grader av konkretisering og detaljering. Hans Petter Graver (1984b): «Sikkerhetsaspekter ved utkastet til ny petroleumslov med forskrifter». I: *Lov og Rett,* s. 140–153. (s. 146).

[140] Ekstern kontroll av internkontrollsystemer er nærmere drøftet i kapittel 4.4.

[141] Et eksempel: «Det kan også gis regler om plikt til å ha internkontrollsystemer og til å føre internkontroll for å sikre at krav fastsatt i eller i medhold av denne lov overholdes.» kommunehelsetjenesteloven, 19. november 1982 nr. 66 § 4a-1(2) annet punktum.

[142] En viktig egenskap ved en rettslig standard er at «dommeren blir henvist til en kjent, utenforliggende målestokk som han skal dømme efter.» Ragnar Knoph (1948): *Rettslige standarder: særlig Grunnlovens § 97*, s. 3.

[143] Ordlyden i helseregisterloven § 16(1): «Den databehandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av helseopplysninger.»

spørsmålet om den ansvarlige faktisk har sørget for tilfredsstillende informasjonssikkerhet kan, i tråd med standardlæren, også fremmes som et rettslig spørsmål.

Et annet behov for fleksibilitet følger av forskjeller i virksomhetenes størrelse og type aktiviteter.[144] En liten virksomhet vil normalt ha mindre kapasitet til å bruke personell-ressurser til internkontroll enn en større virksomhet i samme bransje. På den annen side kan det være enklere å få gjennomført ulike tiltak, som for eksempel sikkerhetsopplæring av ansatte og hensiktsmessig avviksrapportering, i den mindre virksomheten. Derfor er dette et annet slag fleksibilitet enn man får ved å angi en rettslig standard for samfunnshensynet.[145]

Et tredje moment er behovet for å holde tritt med den teknologiske utviklingen. Dette er et viktig rasjonale bak internkontroll. Til dels følger det implisitt av å bruke en rettslig standard for å angi samfunnshensynet. Oppfatningen av hva standarden innebærer kan endre seg over tid.[146] Det forekommer også, selv om det er mer sjelden, at krav til å dra nytte av den teknologiske utviklingen uttrykkes eksplisitt i lov eller forskrift.[147]

Den fjerde og siste formen for fleksibilitet er graden av aksept for feil og avvik. En reell aksept av feil og avvik bør man selvfølgelig finne i ethvert system som involverer mennesker. Også tradisjonelle strafferettslige begreper som overlegg, forsett og uaktsomhet springer ut fra et utgangspunkt om at det ikke nødvendigvis er noens skyld at noe ugreit har inntruffet. Særkjennemerket for internkontroll er, igjen, aktivitetsplikten. Toleransen for avvik skal vurderes og fastlegges. Avvik som ikke ligger innenfor det akseptable skal håndteres etter besluttede prosedyrer. I internkontrollsjargong kalles det «å lukke avviket», som i praksis kan spenne over alt fra å beklage det inntrufne til innskjerping av medarbeideres handlingsrom, omfattende omorganisering eller nyinvesteringer.

---

[144] Et eksempel på en slik formulering finnes i helseforskningsloven § 6(2): «Det skal føres internkontroll tilpasset virksomhetens størrelse, egenart, aktiviteter og risikoforhold.»

[145] Lignende former for fleksibilitet har eksistert i lovverket lenge før internkontrollreformen. Arbeidervernloven fra 1956 hadde et slikt forbehold i plikten til å kunne gi førstehjelp ved ulykker og sykdom: «Nødvendige tiltak avpasset etter arbeidsplassens størrelse, beliggenhet, arbeidets art og de forhold som arbeidet drives under, skal tas for å kunne gi førstehjelp ved ulykker eller sykdomstilfelle.» arbeidervernloven [1956], 7. desember 1956 nr. 2, (Opphevet) § 5(2)(7).

[146] Hensynet til å holde tritt med utviklingen i positive muligheter for å forbedre arbeidsmiljøet ble nevnt i internkontrollutredningen, som et argument *mot* å kvantifisere mål: «En kvantifisering vil også kunne føre til en fastfrysing av kravene til arbeidsmiljøet på det nivå det er mulig å legge seg på i dag, og dermed motvirke den stadig streben etter forbedringer som ligger innebygget i arbeidsmiljøloven.» NOU 1987:10, s. 54.

[147] Det kanskje klareste eksemplet er bestemmelsen som åpner petroleumslovens sikkerhetskapittel: «Petroleumsvirksomheten skal foregå slik at et høyt sikkerhetsnivå kan opprettholdes og utvikles i takt med den teknologiske utvikling.» petroleumsloven [1996], 29. november 1996 nr. 72 § 9-1.

Det rettskildemessige belegget for virksomhetenes handlingsrom til selv å definere toleransen for feil og avvik ligger oftest ikke helt klart oppe i dagen. Det følger snarere av den generelle systematikken.[148]

Det finnes altså flere måter å uttrykke fleksibel regulering på, og det er ikke på noen måte eksklusivt for risikobasert internkontroll som reguleringsmetode. Likevel er det noen nyanser i hva denne fleksibiliteten brukes til: I det idealtypiske internkontrollsystem har hver virksomhet både plikt og rett til å utøve en betydelig grad av normsetting selv. Virksomhetenes muligheter for normsetting går lenger enn bare å være en plikt til oppfatte og rette seg etter påbud, forbud og signaler fra regulerende myndigheter.

Fleksibel regulering er imidlertid ikke nødvendigvis en entydig trend, som til en hver tid øker i omfang. En britisk, empirisk undersøkelse av ulike reguleringer, basert på tekniske standarder for kvalitetssikring, dokumenterer en utviklingstendens som nærmest går i motsatt retning. I flere tilfeller ble regulering som var åpen og fleksibel i utgangspunktet konkretisert og strammet til etter hvert.[149]

4.1.3 Behovet for kontinuitet

Både i Norge og internasjonalt har krav om risikobasert internkontroll, eller beslektede former for regulering, ofte vært utløst av en *cause celebre,* en ulykke, skandale eller krise av stort omfang.[150] Utløsende hendelser har vært av ulik art, fra ulykker i industri og samferdsel, via kvalitetssvikt i næringsmidler og helsetjenester, til økonomiske skandaler eller kriser som har veltet store virksomheter. Et fellestrekk for slike situasjoner på ulike samfunnsområder er

[148] Noen eksempler fra personopplysningsforskriftens sikkerhetskapittel tydeliggjør dette handlingsrommet, selv om det er fordelt ut over litt forskjellige deler av forskriftsteksten. Hovedregelen er at virksomheten selv fastlegger kriteriene: «Det skal føres oversikt over hva slags personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger», § 2-4(1). Videre stilles det krav til en prosess for å behandle avvik. Formålet er spesifisert, men selve prosessen er ikke detaljregulert: «Bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik», § 2-6(1) og «[a]vviksbehandlingen skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse», § 2-6(3). Virksomhetenes handlingsrom for å velge akseptnivå er imidlertid ikke ubegrenset. I tillegg til den generelle begrensningen som ligger i hjemmelslovens rettslige standard «tilfredsstillende informasjonssikkerhet», ligger det også en sikkerhetsventil i tilsynsorganets adgang til å overprøve virksomheter gjennom konkret pålegg: «Datatilsynet kan gi pålegg om sikring av personopplysninger og herunder fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger», § 2-2.

[149] Årsakene til innsnevringer av de opprinnelig fleksible reglene er, ifølge intervjuer i undersøkelsen som det refereres til, at tilsynsorganer ikke har tilstrekkelig tillit til den enkelte virksomhet som fortolker. Forskernes oppsummering er elegant, men trist: «The problem is that regulations are born principled but die detailed.» Paul Skidmore m. fl. (2003): *The Long Game. How Regulators and Companies Can Both Win*, s. 81–82.

[150] Grundig dokumentert blant annet i Laura F. Spira og Michael Page (2003): «Risk Management: The Reinvention of Internal Control and the Changing Role of Internal Audit». I: *Accounting, Auditing & Accountability Journal,* s. 640–661, og i Michael Power (2004): *The Risk Management of Everything: Rethinking the Politics of Uncertainty*. Et par norske eksempler på det samme følger senere i dette kapitlet.

behovet for kontinuitet. Samfunnet vil og må opprettholde en rekke typer virksomhet som drives under en viss risiko. Et internkontrollsystem skal ivareta mål og samfunnshensyn som ikke er omfattet av absolutte krav, der det må eller bør aksepteres feil og avvik. Man må under de aller fleste omstendigheter, også ved relativt alvorlige feil, anta at virksomheten skal fortsette. Dette kan ses som en underliggende premiss for internkontroll, og for statlig tilsyn med virksomheters internkontrollsystemer, men det er vanligvis ikke tydelig uttrykt i rettskildene. Hensynet til kontinuitet kan være en bakenforliggende årsak til forsiktighet med, eller ikke-bruk av, tilsynsorganers sanksjonshjemler.

Behovet for kontinuitet er også lite omtalt i faglitteratur om internkontroll. En mulig grunn kan være at behovet for kontinuitet virker som en ren selvfølgelighet, som det ikke er nødvendig å peke på. Det kan imidlertid oppstå dilemmaer mellom kontinuitet og andre ønskede effekter av en sanksjon. Ett dilemma er at sanksjonen i seg selv kan bli så byrdefull at virksomheten den rettes mot ikke har evne til å rette seg etter pålegg og fortsette driften. Et annet dilemma er at forsiktig bruk av sanksjoner, for ikke å ramme kontinuiteten i nødvendig virksomhet, er at tilsynsorganet kan fremstå som handlingslammet og tape legitimitet og autoritet. For et tilsynsorgan kan det tenkes at tilliten i befolkningen styrkes mer av å demonstrere en evne til «å luke ut råtne epler» enn å la virksomheter lære av egne avvik over tid.

4.1.4 Beslektede metoder i utenlandsk regulering og rettsteori

Risikobasert internkontroll, i varianter som ligger relativt nær den idealtypen som er beskrevet ovenfor, er også utbredt internasjonalt.[151] Internkontroll kan i utgangspunktet dreie seg om både pålagte aktiviteter, og om frivillige prosesser, som virksomheter velger å innføre ut fra egennytte. Internkontroll som ikke er pålagt kan også i en del sammenhenger være gjenstand for ekstern kontroll, gjennom sertifiseringsordninger knyttet til tekniske standarder og lignende.[152] Det har imidlertid vært en stigende tendens, i en rekke land, til økt formalisert regulering av denne typen.

---

[151] En bred og i store trekk kritisk gjennomgang av denne utviklingen, primært med eksempler fra Storbritannia, finnes i Power (2004). Forfatteren trekker en klar forbindelseslinje mellom internkontroll som reguleringsmetode og mer generelle betraktninger om en del gjennomgripende egenskaper ved risikosamfunnet: «A conspicuous feature of the risk management of everything has been the rise of the internal control system. Such systems translate primary or real risks into systems risks» (sitert fra side 24).

[152] Et spesielt relevant eksempel her er den toneangivende standarden innen generell informasjonssikkerhet, NS-ISO/IEC 17799:2005 Administrasjon av informasjonssikkerhet». En tidligere utgave av denne standarden ligger til grunn for sikkerhetskapitlet (kapittel 2) i personopplysningsforskriften, som er grunnlaget for Datatilsynets tilsyn med sikring av personopplysninger i norske virksomheter. Private eller offentlige virksomheter som ønsker det kan imidlertid også velge å la seg sertifisere, for eksempel av Det Norske Veritas, etter nevnte ISO-standard.

For å få et klarere bilde av utbredelsen internasjonalt er det også nødvendig å se på andre teorier og begrepsdannelser som er nært beslektet med internkontroll.[153] Håndhevet selvregulering, refleksiv rett og metaregulering er ulike begreper som beskriver dynamisk regulering, der virksomhetenes egne prosesser for å styre seg selv integreres med og reflekteres i den formelle reguleringen fra samfunnet utenfor virksomheten. Også andre beslektede teorier og begrepsdannelser kunne ha vært føyd til listen. En engelsk samlebetegnelse som av og til brukes om disse reguleringsmetodene, og som understreker at det er en slags familie av teorier med noen fellestrekk, er «lighter-touch regulations».

Én måte å forstå disse reguleringsformene på, som ligger nærmere konvensjonelle rettslige begreper, er at de innebærer en omdanning fra materielle til prosessuelle regler. Det kan ses som en mulig strategi for å kunne håndtere kompleksitet og forskjellighet innenfor et rettslig rammeverk. For eksempel er det relativt abstrakte systemteoretiske begrepet refleksiv rett tolket som uttrykk for at en slik omdanning skjer i et betydelig omfang.[154] Teubner trekker også selv linjene mellom refleksiv rett og internkontroll som reguleringsmetode, i et bokkapittel om metoder for å operasjonalisere og regulere virksomheters samfunnsansvar:

> Could this not even be the point – not where the law ends (Stone, 1975), but where the law begins: «reflexive» control of corporate behavior – by transforming external social problems into internal political issues of the enterprise? The law would have to begin then with the deliberate design of organizational structures which make the corporation sensitive to the external effects of its maximizing its internal rationality. The main function of the law would thus be to substitute outside interventionist control by an effective internal control structure, *to design structural preconditions for an «organizational conscience» that would reflect the balance between its social functions and its environmental performance* – this would determine the integrative role of law in regard to CSR.[155]

[153] Blant de begrepene som er mest teoretisk gjennomarbeidet er *håndhevet selvregulering*, jf. Ian Ayres og John Braithwaite (1992): *Responsive Regulation: Transcending the Deregulation Debate*; John Braithwaite (1982): «Enforced Self-Regulation: A New Strategy for Corporate Crime Control». I: *Michigan Law Review,* s. 1466–1507, *refleksiv rett,* jf. Günther Teubner (1983): «Substantive and Reflexive Elements in Modern Law». I: *Law and Society Review,* s. 239–285 og *metaregulering,* jf. Colin Scott (2003): «Speaking Softly Without Big Sticks: Meta-Regulation and Public Sector Audit». I: *Law & Policy,* s. 203–219.

[154] Julia Black (2000): «Proceduralizing Regulation: Part I». I: *Oxford Journal of Legal Studies,* s. 597–614, påviser denne generelle trenden, gjennom flere eksempler på endret regulering der materielle regler erstattes av prosessuelle regler. Artikkelen knytter utviklingen til teori om regulering av selvreguleringsprosesser. Teorien som brukes er grunnleggende basert på begrepet refleksiv rett, med en tolkning som ligger relativt nær idealtypen risikobasert internkontroll slik den er konstruert her.

[155] Günther Teubner (1985): «Corporate Fiduciary Duties and Their Beneficiaries: A Functional Approach to the Legal Institutionalization of Corporate Responsibility». I: *Corporate Governance and Directors' Liabilities. Legal, Economic and Sociological Analyses on Corporate Social Responsibilities*. (s. 166, original utheving). Forkortelsen «CSR» i sitatet står for Corporate Social Responsibility.

Henvisningen til Stone, 1975 i sitatet ovenfor viser til et amerikansk rettspolitisk arbeid, der selvregulering begrunnes ut fra at det vil være nødvendig for å håndheve virksomheters oppfyllelse av ulike samfunnshensyn. De sentrale argumentene er for det første at kostnadene ved å håndheve lover i tradisjonell forstand er for store i denne typen spørsmål. For det andre vil håndhevelsen av slike plikter ofte komme i konflikt med høyere verdier i samfunnet. Det tredje argumentet er at normene for adferd eller etiske standarder vanskelig lar seg oversette til rettslige standarder som er egnet for domstolsbehandling.[156]

Regulering som i store trekk ligner idealtypen risikobasert internkontroll, er en av flere mulige måter å implementere regulering av selvreguleringsprosesser på. Denne familien av teorier omfatter således atskillig flere reguleringsformer enn den idealtypen som er konstruert her. De fellesnevnerne som er viktigst i denne sammenhengen er respekt for virksomhetens handlingsrom, kombinert med en aktivitetsplikt som sikrer at virksomhetene faktisk gjennomfører dette, og kan gjøre rede for hvilke regler de har «gitt seg selv».

4.2 To historiske linjer: Forskjellige samfunnshensyn og varianter av metoden

Risikobasert internkontroll som reguleringsmetode kom i utgangspunktet inn i lovgivningen som en reguleringsmetode som ga stor plass til faglig og teknologisk ekspertise. Det er en måte å håndtere kompleksitet på, som forutsetter at virksomheter må kunne fremvise, begrunne og forsvare sitt eget arbeid med å avhjelpe de problemer virksomheten skaper. Metoden ble imidlertid også, relativt kort tid etter at den først kom inn i lovgivningen, vurdert som egnet for å ivareta flere ulike typer samfunnshensyn. Det er en reguleringsmetode som har vært, og er, i stadig endring. Det har også utviklet seg forskjellige varianter av metoden, med større eller mindre avstand til den idealtypen som er konstruert her.

[156] Christopher D. Stone (1975): *Where the Law Ends: The social control of corporate behavior*. Samme forfatter presiserer også selvreguleringsaspektet i et senere essay om virksomheters samfunnsansvar: Christopher D. Stone (1985): «Corporate Social Responsibility: What It Might Mean, If It Were Really to Matter». I: *Iowa Law Review,* s. 557–575.

4.2.1 Internkontroll før begrepet kom inn i norsk lovgivning

Internkontrollens historie går lenger tilbake enn de få tiårene det har vært knyttet til en del bestemmelser i norsk lovgivning.[157] Den historiske utviklingen av internkontrollbegrepet illustrerer godt hvor åpen og fleksibel denne reguleringsmetoden har vært for tilpasning til nye behov.

Internal controls utviklet seg i USA fra en uformell terminologi, via formelle definisjoner, til et mer omfattende metodisk rammeverk. De følgende punktene fra den historiske utviklingen på området er i hovedsak basert på en artikkel som beskriver en langvarig kontrovers i USA, om hvorvidt revisorer bør gi en vurdering av de reviderte virksomheters internkontrollsystem.[158] Fra tidlig på 1900-tallet tilrådde faglige anbefalinger om revisjon å gi en vurdering av hvor gode systemer for internkontroll den reviderte virksomheten har. Hensikten var kun praktisk, det skulle være til hjelp når man tok stilling til hvor stort omfang det var nødvendig å gi den detaljerte regnskapskontrollen. I 1948 definerte American Institute of Accountants begrepet slik:

> Internal control comprises the plan of organization and all of the co-ordinate methods and measures adopted within a business to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies.[159]

Denne definisjonen, særlig det siste punktet om tilslutning til ledelsens policyer, pekte frem mot et videre mål for kontrollene enn ren regnskapskontroll. En slik utvidelse fikk både tilhengere og motstandere. Noe av det man var engstelig for, var at revisoren kunne bli ansvarlig for usikre vurderinger langt utenfor sitt egentlige fagfelt. Et forsøk på å løse dette problemet motiverte en ny anbefaling i 1958, som trakk et skille mellom administrativ og regnskapsmessig internkontroll. I utgangspunktet skulle ikke revisjonsberetningen vurdere den administrative internkontrollen, men revisoren kunne ta den i betraktning ved mistanke om at den hadde vesentlig betydning for den regnskapsmessige kontrollens pålitelighet.

De følgende tiårene, fremdeles i USA, svingte pendelen frem og tilbake mellom et smalt regnskapsperspektiv og et helhetlig styringsperspektiv. Fra slutten av 1980-tallet begynner imidlertid internkontroll som styringsprosess å slå gjennom for fullt. I 1988 var anbefalingen

[157] Dette fremgikk også av forarbeider til den store internkontrollreformen innen arbeidsmiljølovgivning: «Begrepet internkontroll stammer opprinnelig fra økonomisk språkbruk.» NOU 1987:10, s. 20. Utrederne sa imidlertid ikke mer om hvilket innhold begrepet har og har hatt i økonomisk språkbruk, og hvor mye dette lignet eller avvek fra deres forslag.
[158] Jan R. Heier m. fl. (2005): «A century of debate for internal controls and their assessment: a study of reactive evolution». I: *Accounting History,* s. 39–70.
[159] Heier m. fl. (2005), s. 48.

at revisor skulle vurdere virksomhetens kontrollmiljø, herunder hvorvidt ledelsens holdninger, aktsomhet og handlinger var i overensstemmelse med deres egne policyer og prosedyrer. Et dokument som raskt fikk stort gjennomslag internasjonalt som rammeverk for virksomheters egne styringssystemer, var «COSO-rapporten».[160] COSO definerer internkontroll som en prosess, som gjennomføres i hele virksomheten fra styre og ledelse til alt øvrig personell. Prosessen skal gi en rimelig sikkerhet for at virksomheten fungerer effektivt, har pålitelig økonomirapportering, og drives i overensstemmelse med de lover og regler som kommer til anvendelse. Like viktig som det store omfanget internkontrollen får ved denne definisjonen, er vektleggingen av en helhetlig risikostyring som metode for både å utforme, gjennomføre og etterprøve virksomhetens styringsmål. COSO-rapporten vektlegger også at dette er et verktøy for virksomheten, oppmerksomheten flyttes fra spørsmålene om revisjonsberetningens omfang til virksomhetens egen nytte av disse prosessene.

Likheten mellom COSO-rapportens anbefalinger og idealtypen risikobasert internkontroll, slik den er konstruert her, er slående. I den forbindelse er det verdt å merke seg kronologien, en god del av den norske lovgivningen om internkontroll er av eldre dato enn COSO. Det viser at COSO, tross sin store innflytelse, ikke egentlig lå i forkant av utviklingen. Man kan kanskje heller se det slik at COSO-rapporten hentet tilbake til økonomiområdet og den generelle virksomhetsstyringen en del av de nye impulsene som internkontrollbegrepet i mellomtiden hadde fått fra mer teknologisk orienterte disipliner som sikkerhetsadministrasjon og kvalitetssikring. Utviklingen av internkontroll som reguleringsmetode har vært og fortsetter å være et resultat av krysspåvirkning mellom ulike samfunnshensyn og reguleringsområder.

4.2.2 Internkontrollreformen i Norge

Sikkerhetsreguleringene for petroleumsvirksomheten på norsk sokkel, og deretter HMS-reguleringen, var tidlige eksempler på rettslig regulering av internkontroll, også i internasjonal målestokk. De er imidlertid, man kan være fristet til å si dessverre, ikke de aller eldste. United States Nuclear Regulatory Commission stilte fra 1970 krav om å dokumentere et omfattende kvalitetssikringssystem, som en forutsetning for konsesjon til etablere og bruke

[160] *Internal Control – Integrated Framework.* (1992). COSO er en forkortelse for *the Committee of Sponsoring Organisations of the Treadway Commission*. Komiteen besto av flere sammenslutninger av økonomieksperter og intern- og eksternrevisorer. James Treadway ledet *the National Commission on Fraudulent Financial Reporting*, som var et uavhengig initiativ fra privat sektor i USA, etablert i 1985.

kjernekraftverk.[161] Innretningen av dette kvalitetssikringssystemet har mange trekk til felles med idealtypen risikobasert internkontroll.

Det første området der Norge lovfestet en plikt til å etablere internkontrollsystemer var petroleumsvirksomheten på norsk sokkel. Både i ordlyd og innretning dreide den første reguleringen på dette området seg overveiende om arbeidstakervern. Denne typen regler var motivert både av konkrete høye ulykkestall, og av at arbeidstakeres vern i offshorevirksomheten var mangelfullt regulert.

Fra slutten av 1970-tallet begynte Oljedirektoratet en ny form for tilsynspraksis overfor rettighetshaverne på norsk kontinentalsokkel. Endringen besto i en overgang fra tradisjonell verifikasjon av at rettighetshaveren har fulgt detaljerte regler som er fastsatt av myndighetene, til å etterprøve at rettighetshaveren har egne systematiske og helhetlige prosesser på plass for å sikre samsvar med mer generelt utformede målsetninger. Oljedirektoratet utarbeidet retningslinjer, i form av et kort dokument, som var på norsk i venstre kolonne og med engelsk oversettelse i høyre kolonne.[162]

Innledningskapitlet i Oljedirektoratets retningslinje fra 1979 henviser til arbeidsgivers plikter etter daværende lov,[163] med presiseringer i forskrifter. Retningslinjen henviste til lovens § 14 første ledd, og bestemmelser vedtatt ved kongelig resolusjon. Hovedinnholdet i disse henvisningene var krav til arbeidstakervern, og plikten til å sørge for at virksomheten ble planlagt, organisert og utført i samsvar med bestemmelsene gitt i loven.[164] Retningslinjen innholdt også presiseringer av rettighetshavers ansvar for å påse at enhver som utfører arbeid for ham, uansett om vedkommende er ansatt, kontraktør eller underkontraktør, overholder bestemmelsene. Denne vektleggingen av et vertikalt ansvar fra rettighetshaver ned til den enkelte var godt synliggjort i retningslinjen.

I en sak som gjaldt arbeidsgivers ansvar for sikkerhetsopplæring la Høyesterett *ikke* Oljedirektoratets retningslinje til grunn.[165] Sakens bakgrunn var ulykken der boligplattformen Alexander L. Kielland veltet, 27. mars 1980. Stavanger politikammer hadde utferdiget et forelegg mot en kontraktør. Politikammeret mente selskapet hadde brutt plikten etter

[161] 10CFR50b (1970): Appendix B to Part 50 – Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.
[162] Oljedirektoratets retningslinjer [1979], 7. juni 1979, (Opphevet). Den norske versjonen brukte ordet egenkontroll i tittelen, mens det i den parallelle engelske teksten het *internal control*. Retningslinjene ble revidert 15. mai 1981, og da var ordet «egenkontroll» erstattet med «internkontroll» også i den norske teksten.
[163] Arbeidsmiljøloven [1977], 4. februar 1977 nr. 4, (Opphevet).
[164] Retningslinjen viste ikke til en positivt angitt hjemmelskjede fra overliggende lov eller forskrift, men bygget på en antakelse om at «sørge for»-pliktene kunne ses som et implisitt internkontrollkrav: «Ovennevnte plikter og ansvar vil bl.a. betinge at rettighetshaver bygger opp et kontroll- og dokumentasjonssystem som skal sikre at bestemmelsene overholdes.» Oljedirektoratets retningslinjer [1979] s. 3.
[165] Rt. 1984 s. 337.

arbeidsmiljøloven § 14 annet ledd bokstav h, til å gi ansatte grunnleggende opplæring om farene ved opphold på plattformen og sikkerhetstiltak i denne forbindelse. Selskapet vedtok ikke forelegget, og ble frikjent i Jæren herredsrett. Høyesterett opprettholdt frifinnelsen. Den ansatte, som ifølge forelegget ikke skulle ha fått tilstrekkelig opplæring, hadde etter Høyesteretts vurdering tilstrekkelig erfaring og kunnskap om farer og sikkerhetstiltak til at selskapet ikke hadde forsømt opplæringsplikten. Høyesterett la til grunn at Oljedirektoratet, som hadde fått kompetanse til å gi forskrifter etter arbeidsmiljøloven på dette området ved kongelig resolusjon, ikke hadde gitt noen forskrifter om sikkerhetsopplæring av personell i offshorevirksomheten. Dermed var de henvist til å avgjøre spørsmålet «direkte på grunnlag av arbeidsmiljøloven § 14 annet ledd bokstav h, uten den veiledning som en forskrift ville ha gitt.»[166]

4.2.2.1 Første plikt til internkontroll i formell lov

Selve ordet internkontroll kom for første gang inn i formell lov med endringslov 25. mai 1984 nr. 31, som blant annet innførte en ny bestemmelse i sjødygtighedsloven.[167] Til tross for klar tilslutning fra sikkerhetsfaglig hold, var politikernes tro på internkontroll blandet med en viss skepsis. I komitéinnstillingen til endringsloven var dette den eneste av endringene sjøfarts- og fiskerikomiteen så grunn til å kommentere.[168] Den konkrete foranledningen til internkontrollplikten i sjødygtighedsloven var tilrådninger som ble gitt i stortingsmeldingen etter Kiellandulykken. Selv om boligplattformen var brukt i petroleumsvirksomheten, hørte forholdet formelt sett inn under sjøfartsreguleringen fordi det var en flytende plattform. En av de anbefalingene som ble gitt for å bedre sikkerheten på denne typen innretninger var å innføre styringssystem for sikkerhetskontroll, i form av en plikt til internkontroll.[169] Med lovendringen i 1984 gjaldt den nye § 9a i sjødygtighedsloven bare flyttbare innretninger knyttet til petroleumsvirksomheten til havs. Senere, ved endringslov 2. august 1991 nr. 70, ble

[166] Rt. 1984 s. 337, på s. 340–341. Denne rettskildesituasjonen ble i neste setning kommentert med følgende hjertesukk: «Det sier seg selv at anvendelsen av en så skjønnsmessig og standardpreget regel på et så spesielt og komplisert arbeidsområde som det her er tale om, stiller domstolene overfor betydelige problemer.»

[167] Sjødygtighedsloven, 9. juni 1903 nr. 7, (Opphevet) § 9a. Opprinnelig ordlyd etter vedtaket i 1984 var «For innretninger som nevnt i § 1 tredje ledd nr. 2 kan Kongen ved forskrift pålegge rederen å etablere et system for internkontroll til sikkerhet for at bestemmelser gitt i eller i medhold av lov eller av godkjent besiktelsesinstitusjon overholdes.» De innretningene det er henvist til i sitatet var flyttbare innretninger i petroleumsvirksomheten.

[168] Selv om komiteen i utgangspunktet stiller seg positiv til bestemmelsen, vil den «imidlertid understreke at et slikt internkontrollsystem kun kan bli et verdifullt supplement, og ingen erstatning for den offentlige sikkerhetskontroll.» Innst.O. nr. 48 (1983-1984), s. 1.

[169] Internkontroll beskrives i meldingen som en helhetlig prosess, «et internkontrollopplegg», som omfatter vurdering av risiko, kriterier for akseptabel sikkerhet, og systematiske tiltak for å sikre at «kvaliteten blir planlagt, oppnådd og vedlikeholdt.» Stortingsmelding nr. 67 (1981-82), s. 89.

rekkevidden utvidet slik at internkontrollplikten etter sjødygtighedsloven begynte å gjelde generelt for skip.[170]

En egen, nyskrevet lov for petroleumsvirksomheten kom først ti måneder etter endringen som innførte plikt til internkontroll i sjødygtighedsloven.[171] Petroleumsloven nevnte ikke internkontroll i sin ordlyd, men departementet understreket i proposisjonen at kravet til forsvarlig virksomhet i lovens § 45 skulle forstås som en plikt til internkontroll.[172] Heller ikke i gjeldende petroleumslov nevnes internkontroll i lovens ordlyd, til tross for betydelige innslag av denne reguleringsmetoden i sikkerhetsbestemmelsene.[173]

4.2.2.2 Arbeidsmiljøloven og den brede internkontrollreformen

Det som kan betegnes som den store internkontrollreformen i Norge kom noen år senere, med endringslov 27. juli 1990 nr. 52. Endringen innførte plikt til å etablere internkontrollsystem i seks ulike lover, med ikrafttredelsesdato 1. januar 1992.[174] Internkontrollutredningen hadde bare foreslått endring i arbeidsmiljøloven, men holdt døren åpen for at metoden kunne være egnet også for annen sikkerhetsregulering.[175] Etter høringsuttalelser kom departementet til at internkontrollforskriften også burde hjemles i andre lover, der plikter om å ivareta miljø og sikkerhet finnes.[176] Både den første generelle internkontrollforskriften,[177] og den gjeldende,[178] er felles for en rekke forskjellige lover og forskjellige kategorier av samfunnshensyn.

I denne lovsaken, i 1990, var Stortinget mindre skeptiske til internkontroll enn de hadde vært da internkontroll første gang ble lovfestet seks år tidligere.[179] Andre forhold som ble drøftet både i proposisjonen og komitéinnstillingen var behov for samkjøring av tilsynsvirk-

[170] Også endringen i 1991 hadde en tragisk ulykke som bakteppe, den ble foreslått av et utvalg nedsatt etter brannen om bord i MS Scandinavian Star 7. april 1990. Internkontrollplikten for skip er videreført i ny lov, skipssikkerhetsloven, dog uten at «internkontroll» nevnes i den nye lovens ordlyd.
[171] Petroleumsloven [1985], 22. mars 1985 nr. 11, (Opphevet). Proposisjonen til petroleumsloven ble imidlertid levert før proposisjonen til endringen i sjødygtighedsloven, de krysset hverandre altså i tid.
[172] «Rettighetshaver plikter derfor å etablere et system for kvalitetssikring (internkontroll) og må kunne dokumentere at gjeldende sikkerhetsbestemmelser overholdes.» Ot.prp. nr. 72 (1982-1983), s. 77.
[173] Petroleumsloven [1996].
[174] De seks lovene det gjaldt var arbeidsmiljøloven [1977], brannfarlighetsloven (Svalbard), 21. mai 1971 nr. 47, (erstattet av lov 14. juni 2002 nr. 20, gjelder nå bare for Svalbard), lov om eksplosive varer (Svalbard), 14. juni 1974 nr. 39, (erstattet av lov 14. juni 2002 nr. 20, gjelder nå bare for Svalbard), brannvernloven, 5. juni 1987 nr. 26, (Opphevet), forurensningsloven, 13. mars 1981 nr. 6 og produktkontrolloven, 11. juni 1976 nr. 79.
[175] Internkontrollutredningen var delt opp i to dokumenter, NOU 1987:10 og NOU 1987:32.
[176] Ot.prp. nr. 48 (1989-1990).
[177] Internkontrollforskriften [1991], 22. mars 1991 nr. 159, (Opphevet).
[178] Internkontrollforskriften [1996], 6. desember 1996 nr. 1127.
[179] Komitéinnstillingen er svært klar i sin tilslutning, den «legger til grunn at de foreslåtte internkontrollsystemer, sammen med en gradvis overgang til mer resultatorienterte regelverk og målstyringsprinsipper, representerer en viktig og nødvendig del av arbeidet med modernisering og effektivisering av statsforvaltningen.» Innst.O. nr. 43 (1989-1990), s. 3.

somheten, medarbeideres medvirkning, og fremdeles en generell advarsel mot å la internkontroll bli et påskudd for svakere oppfølging av sikkerheten fra myndighetenes side.

Internkontrollreformens største og synligste endring var dens inntog i arbeidsmiljøloven.[180] Plikten til internkontroll har etter det berørt et stort flertall av norske virksomheter. I gjeldende arbeidsmiljølov forekommer ikke lenger «internkontroll» i lovens ordlyd.[181]

4.2.3 Internkontroll for å regulere forskjellige samfunnshensyn

De mange samfunnshensynene kan deles inn i noen få, brede kategorier. Her er de delt inn i seks kategorier. Det er noen uskarpe grenser mellom enkelte av kategoriene, og inndelingen er på ingen måte den eneste som vil være brukbar. Oppstillingen av disse seks kategoriene er valgt av to grunner. Den ene grunnen er at de til dels er dekket av begreper som allerede brukes i litteratur og samfunnsdebatt. Den andre er noen fellestrekk i måten de avviker fra idealtypen på.

De to første kategoriene er introdusert ovenfor, *økonomi og virksomhetsstyring* under begrepets historie, og *arbeidstakervern* under internkontrollreformen i Norge.

Tredje kategori er *samfunnssikkerhet og sårbar infrastruktur*. Kategorien defineres av hvor alvorlige konsekvensene vil være dersom samfunnskritisk virksomhet stanser eller blir alvorlig hindret. Selv om det er mange innslag av plikter til internkontroll, er samfunnets sårbarhet også ofte en begrunnelse for å sette grenser for den enkelte virksomhets handlingsrom til å beslutte mål og midler selv.

Etter den forsiktige begynnelsen i Oljedirektoratet var Statens sprengstoffinspeksjon det andre statlige tilsynsorganet som begynte med kontroll av tilsynsobjektets internkontrollsystem.[182] Sprengstoffinspeksjonens retningslinje hadde en definisjon av internkontroll som ligger nær opp til noen av de idealtypiske trekkene, blant annet organisering, dokumentasjon, korrigering og sykliske forbedringsprosesser. Den tar imidlertid ikke utgangspunkt i virksomhetenes egne risikovurderinger og egen aksept av risiko.

---

[180] Arbeidsmiljøloven [1977] fikk en ny § 16a: «Kongen gir nærmere regler om internkontroll og internkontrollsystemer for å sikre at krav fastsatt i eller i medhold av denne lov overholdes.» Endringer ble også gjort i lovens §§ 24 og 26, for å sikre at internkontrollsystemer var omfattet av arbeidstakernes medbestemmelsesrett.

[181] Någjeldende lov er arbeidsmiljøloven [2005]. Selv om ordet internkontroll ikke nevnes, er det en rekke krav til internkontrollaktiviteter som påligger arbeidsgiver i § 3-1, der overskriften er «krav til systematisk helse-, miljø- og sikkerhetsarbeid». Internkontrollforskriften [1996] ble videreført med den generelle bestemmelsen i lovens § 20-2 om at forskriftene gitt i medhold av forrige arbeidsmiljølov gjelder inntil annet er bestemt.

[182] Sprengstoffinspeksjonens tilnærming var å teste ut denne reguleringsformen i liten skala, hos enkelte tilsynsobjekter, basert på en konkret avtale med hver virksomhet som ville prøve det ut. De utarbeidet en retningslinje, som nærmest fremsto mer som en forklaring av metoden enn som regeltekst. Internkontrollforskrift brannfarlig vare, 7. desember 1982 nr. 3442. (Opphevet).

I de senere årene er det særlig innen området terrorbekjempelse at handlingsrommet for den enkelte virksomhet har blitt vesentlig beskåret.[183] Fremveksten av felles europeisk politikk for terrorbekjempelse har synliggjort, og kanskje forsterket, noen faglige motsetninger mellom ulike sektormyndigheters syn på denne reguleringsmetoden. Samfunnssikkerhetens problem ligger ofte i at sårbarheten gjelder forhold utenfor de enkelte virksomhetene, og derfor ikke blir fanget opp i de interne prosessene for å identifisere risiko. Faren ligger ikke i at virksomhetene kan misbruke handlingsrommet til å forfølge egeninteresser, men i at man ikke kan være sikker på om virksomhetens oppriktige og samvittighetsfulle internalisering av samfunnshensynet fører til relevante tiltak.[184]

Deler av idealtypen risikobasert internkontroll inngår likevel fremdeles i reguleringen av samfunnssikkerhetshensynene. Plikter for den enkelte virksomhet følger ofte et lignende mønster selv om det handlingsrommet som ligger i å basere tiltak og kontroll på egne vurderinger av risiko snevres inn.

Fjerde kategori er *naturressurser, næringsmidler og miljøvern*. For denne kategorien samfunnshensyn utgjør plikter til internkontroll ofte en begrenset del av de rettslige virkemidlene, de virker sammen med blant annet konsesjonssystemer og detaljregler. Det er imidlertid mange bestemmelser om internkontroll innen disse samfunnshensynene, og de ligger relativt nær opptil den konstruerte idealtypen. Innen disse samfunnshensynene finnes

[183] Et eksempel er sikring av havner. Regelverket har beholdt deler av internkontrollmetodikken, men det er relativt nylig utvidet med en rekke detaljerte krav med lite slingringsmonn. Bakgrunnen for disse endringene er Rfo 725/2004/EF. I stedet for det enkelte havneanleggs egen vurdering og aksept av risiko, skal sikkerhetstiltakene ta utgangspunkt i sentraliserte, løpende vurderinger av trusselbildet. Forordningen er gitt denne form i norsk forskrift: «Objektene skal tilpasse sikringstiltakene til det sikringsnivå som til enhver tid er fastsatt av norske myndigheter.» forskrift om sikring av havner mot terror, 3. juli 2007 nr. 825 § 14. Sårbarhetsvurdering for det enkelte havneanlegg skal enten Kystverkets regionkontor eller en uavhengig virksomhet godkjent av Kystverkets hovedkontor utføre.

[184] En nokså skarp kollisjon mellom synet på hvorvidt reguleringen skal ta utgangspunkt i virksomhetens egne vurderinger eller eksterne vurderinger kom relativt nylig til overflaten i Justisdepartementets og Direktorat for samfunnssikkerhet og beredskaps reaksjoner på Petroleumstilsynets forslag til nytt, helhetlig regelverk for petroleumsvirksomhet, som også skulle omfatte en del landanlegg (høringsdokument 22. august 2008, Justis- og politidepartementets høringssvar av 4. desember 2008). Petroleumstilsynets tilnærming til sikring av eksplosiver var risikobasert internkontroll, for å oppnå sikkerhet mot ulykker og andre alvorlige konsekvenser av feilhåndtering i den enkelte virksomhet som håndterer eksplosivene. Justisdepartementet peker på at forslaget ikke tar inn over seg «de stadig strengere krav til sikkerhet mot at eksplosiver kommer på avveie», med henvisning til utviklingen i EU, de siktet formodentlig til anbefalingene i KOM(2007) 651, «Meddelelse fra kommisionen om øget sprængstofsikkerhed». I tiltakene mot at eksplosiver kommer på avveie er detaljregulering av aktørene, samlete oversikter, kontroll med eksplosiver som skal avhendes, og sentral kunnskap om avvik, viktigere enn å forankre reguleringen i lokal kunnskap og oppfølging i den enkelte virksomhet. Sentrale tiltak mot sprengstoff på avveie er også et av de konkrete tiltakene mot terror som er omtalt i Stortingsmelding nr. 22 (2007-2008), s. 36. Departementets høringsuttalelse var også svært skarp i kritikken av Petroleumstilsynets forslag til en teknikk for å innarbeide Direktorat for samfunnssikkerhet og beredskaps gjeldende regelverk for de aktuelle landanleggene. Teknikken vurderes som «uakseptabel ut fra et sikkerhetsmessig synspunkt».

det også enkelte varianter av internkontrollprinsippet som kan ses som en innsnevring av virksomhetens eget handlingsrom i arbeidet med å vurdere risiko.[185]

Femte kategori er *produktsikkerhet.* Internkontrollsystemene her er ofte knyttet til tekniske standarder. Selv om produktkontrolloven var med i den brede internkontrollreformen som trådte i kraft i 1992, kom det relativt kort tid etter omfattende endringer som følge av EØS-avtalen.[186] Det er en stor mengde ulike standarder som regulerer sikkerheten i forskjellige produkter, detaljeringsgraden i standardene er sterkt varierende. Innen mange bransjer gjelder standarder som ligger nær idealtypen risikobasert internkontroll, altså slik at standarden i seg selv nærmest bare er prosessregler om håndtering av risiko. I andre bransjer kan standardene være detaljert ned til en samling konkrete sjekklister. I begge tilfeller er forbrukernes møte med denne reguleringsmetoden symbolet CE, som en lang rekke produkter er merket med.

Den sjette kategorien samfunnshensyn, som er mest aktuell for avhandlingens problemstilling, kan gis merkelappen *forsvarlighet, rettssikkerhet og individers rettighetsvern*. Til forskjell fra arbeidstakervern gjelder dette hovedsakelig interessene til enkeltindivider utenfor virksomheten; brukere, kunder, klienter og pasienter. Forsvarlighet, rettssikkerhet og individers rettighetsvern skiller seg også fra produktsikkerhet, der sikkerhetsegenskapene skal være objektive ut fra en standard. Denne kategorien hensyn dreier seg om hvilke konsekvenser virksomhetens valg, prioriteringer, aktsomhet og ferdigheter får for enkeltpersoner. Det virker antakelig fremmedartet å klassifisere individers rettighetsvern som samfunnshensyn. Mer vanlig er det nok å se samfunnshensyn og individuelle rettigheter som motpoler, der det er behov for å veie interesser mot hverandre. I tillegg vil det oftest være andre, og mer konkrete, lovbestemmelser som regulerer de aktuelle pliktene og rettighetene. Grunnen til at det likevel tas med som en kategori samfunnshensyn her, er at forsvarlighetsnormer,

[185] Det gjelder særlig føringene om bruk av kritisk kontrollpunkt-analyse som metodisk tilnærming til risikovurderingen, internkontrollforskriften for næringsmidler, 15. desember 1994 nr. 1187 § 5a (forskriften har det uformelle tilnavnet «IK-mat»). I internasjonal faglitteratur kalles metoden HACCP, en forkortelse for Hazard Analysis and Critical Control Point. Metoden styrer risikohåndteringen inn mot noen få, kjente problemområder. Dette skal bidra til mer objektiv og etterprøvbar risikoforståelse, mens kostnaden er en fare for at konkrete risikomomenter som ligger utenfor de definerte kontrollpunktene ikke blir fanget opp.

[186] EU vedtok en resolusjon 7. mai 1985 (85/C 136/01) om ny metode («new approach»). I bilag II til denne resolusjonen – «retningslinjer for en ny metode i forbindelse med teknisk harmonisering og standarder» – er det angitt noen grunnleggende føringer for den nye metode. De tekniske spesifikasjonene skal ha status som frivillige standarder, men offentlige myndigheter har fortsatt det fulle ansvar for sikkerheten. Samsvar med produktsikkerhetskravene kan kontrolleres av ulike ikke-offentlige organer, som er utpekt av relevant myndighet. Reglene om utpeking av norske kontrollorganer følger av lov om tekniske kontrollorgan, 16. juni 1994 nr. 20. EU og EØS-landene er forpliktet til gjensidig anerkjennelse av hverandres utpekte kontrollorganer for samsvarsvurdering. (Oversikt over hvilke slike kontrollorgan som er utpekt, og hvilket eller hvilke direktiver organet dekker, finnes i det offentlig tilgjengelige Nando Information System. Nando er et akronym for New Approach Notified and Designated Organisations).

prosessuelle regler og rettigheter for individer i noen tilfeller er «støpt om» til et hensyn som skal ivaretas gjennom virksomheters plikt til risikobasert internkontroll.

Individers rettighetsvern, betraktet som et hensyn virksomheten skal ivareta gjennom å utøve internkontroll, har visse problematiske sider. Det som en virksomhet definerer som en akseptabel risiko kan oppleves som vilkårlig, arrogant eller uakseptabelt av det enkelte individ som virksomheten har ment å gi et tilstrekkelig vern. Dessuten er statlige tilsynsorganers sanksjonsapparat i liten grad utformet for å sikre konkret rettferdighet for den enkelte. Et av samfunnshensynene i denne kategorien er personopplysningsvern, der internkontroll er metoden for å sikre at den ansvarlige er i stand til å imøtekomme og overholde den registrertes rettigheter. Innen helsetjenesten er medisinsk forsvarlighet det overordnede hensynet som internkontrollen skal ivareta. Tiltak som er mer spesifikt rettet mot å ivareta den enkelte pasients rettighetsvern utgjør en avgrenset del av pliktene til internkontroll.[187] Andre eksempler på hensyn i denne kategorien er forsvarlighet og brukeres trygghet og rettigheter i barnehager og barnevernsinstitusjoner med mer.

Pliktsubjektene for mange av samfunnshensynene i denne kategorien er offentlige etater, eller tjenestetilbydere som utfører oppgaver på vegne av offentlige etater. Med helseregisterlovens og personopplysningslovens plikter til internkontroll er imidlertid også et stort antall private virksomheter omfattet.[188]

4.2.4 Flere varianter av reguleringsmetoden

Internkontroll som reguleringsmetode har ikke hatt en fasttømret og stabil form fra starten til i dag. Reguleringsmetoden er fleksibel, ikke bare i den betydning at den kan gi den enkelte virksomhet stort handlingsrom, men også slik at metoden i seg selv har vært formbar. Fra en viss formalisering der begrepet oppsto, på økonomiområdet, har internkontroll senere tatt opp i seg kvalitetssikringsmetodikk og et risikohåndteringsparadigme. På vei inn, i et omfang som foreløpig er vanskelig å fastslå, er den sterkere vektleggingen av tiltak for terrorbekjempelse. Det er et utviklingstrekk som kan innebære styrket ekstern kontroll med at samfunnshensynene ivaretas også utenfor virksomhetens fysiske og regulatoriske vegger. Imidlertid er det

[187] I Helsedirektoratets veiledning om internkontroll, *Hvordan holde orden i eget hus: Internkontroll i sosial- og helsetjenesten.* (2009), er internkontrollsystemet fremstilt som redskap for å ivareta alle typer myndighetskrav.
[188] Personopplysningsloven, inneholder i realiteten to separate plikter til internkontroll. Den ene ligger i kravene til planlagte og systematiske tiltak for informasjonssikkerhet (§ 13), den andre i kravene til internkontrollsystem for å sikre at lovens øvrige plikter og rettigheter ivaretas og etterleves (§ 14). De tilsvarende bestemmelsene i helseregisterloven finnes i henholdsvis §§ 16 og 17. Individers rettighetsvern som samfunnshensyn er primært knyttet til personopplysningsloven § 14 og helseregisterloven § 17.

mye igjen av de idealtypiske metodetrinnene også på de områdene der økt ekstern kontroll fører til at virksomhetenes handlingsrom innskrenkes.

Ovenstående gjennomgang av noen korte og fortettede trekk ved utviklingen og utbredelsen av internkontrollregulering viser at reguleringsmetoden finnes i ulike varianter, som i forskjellig grad ligner eller avviker fra den konstruerte idealtypen. Man kan dele inn dette i fire «reguleringsmetodiske varianter».[189] Den første, og opprinnelige, varianten kan kalles revisjonsperspektivet. Under dette perspektivet er internkontroll først og fremst etterprøving, uten at en eventuell rett eller plikt til normsetting har særlig relevans. Den andre varianten kan kalles kvalitetssikringsperspektivet, som særlig bygger på to grunnleggende prinsipper. Det ene er sykliske forbedringsprosesser, altså en metodisk tilnærming til å lære av tidligere feil. Det andre er et nærhetsprinsipp, fastleggingen både av hva som skal kontrolleres og hvordan det skal kontrolleres bør ligge nærmest mulig de som utfører arbeidet. Tredje variant er den helhetlige risikohåndteringen, med høy grad av suverenitet for den enkelte virksomhet. Idealtypen risikobasert internkontroll, slik den er konstruert her, er i hovedsak basert på denne tredje varianten, men den har også betydelige innslag av kvalitetssikringsvarianten. I den fjerde varianten, som kanskje særlig kommer til syne i tiltakene for terrorbekjempelse, er det lagt større vekt på horisontal kvalitet, sikkerhet og kontroll på tvers av virksomhetene. Det innebærer en delvis reversering av virksomhetenes eget handlingsrom.

Selv om utviklingen av disse fire variantene av internkontroll for så vidt har fulgt en slags kronologisk rekkefølge, er det ikke slik at de avløser hverandre. Reguleringene består, og utvikles til dels hver for seg. Alle variantene finnes side om side. Resten av kapitlet belegger at virksomheters behandling og sikring av helseopplysninger er basert på regulering som ligger nær opp til idealtypen risikobasert internkontroll, og drøfter noen fordeler og dilemmaer knyttet til det.

4.3 Nærmere om de enkelte idealtypiske metodetrinnene

4.3.1 Organisering av virksomhetens internkontrollarbeid

I de fleste forskriftsbestemmelser om internkontroll stilles det krav om å dokumentere organiseringen av internkontrollarbeidet i virksomheten. Dette er ofte et rent dokumentasjonskrav, bare i relativt beskjeden grad legger regelverket føringer for organiseringen. Kravet

[189] Inndelingen i fire varianter er temmelig grovmasket, og eksisterer bare her som et analytisk grep. Dersom man går nærmere inn i detaljene i det enkelte regelverk måtte antallet «varianter» settes atskillig høyere.

til å dokumentere organiseringen er et tydelig identifiserbart metodetrinn, som har en lang historie i litteratur og regelverk om internkontroll. For å bruke noen eksempler blant de tidlige forekomstene som allerede er omtalt, finner man eksplisitte krav til å dokumentere organiseringen i den første definisjonen av internkontroll i den amerikanske anbefalingen for revisorer fra 1948, i kravene til sikkerhet og kvalitetssikring i amerikansk atomkraftregulering fra 1970, i Oljedirektoratets retningslinje fra 1979, og i Sprengstoffinspeksjonens retningslinjer for internkontroll fra 1982.

Til tross for at organisering har vært et sentralt element i hele internkontrollens historie, er det vanskelig å få øye på noen uttalt begrunnelse for dette. Organisering synes å være det minst diskuterte, og minst begrunnete, av metodetrinnene i litteraturen. Man kan likevel gjøre noen antakelser om hvilke formål dokumentasjonen kan ha. For det første vil en beskrivelse av hvordan internkontrollarbeidet er organisert bidra til å identifisere oppgavene, slik at de er synlige i planer, budsjetter og i ledelsens agenda ellers. Et mer praktisk hensyn er at dokumentasjon av organiseringen formodentlig letter eksterne tilsynsorganers arbeid med å orientere seg og planlegge sitt arbeid.

To andre momenter er kanskje likevel viktigere for en teoretisk analyse av internkontroll som reguleringsmetode. Det ene er at dokumentasjonskravet tvinger virksomheten til å velge mellom hvorvidt internkontroll skal organiseres som en egen funksjon ved siden av den primære forretnings- eller forvaltningsvirksomheten, eller om arbeidet skal integreres tettere med primære funksjoner. Det andre momentet er om virksomheten organiserer og utøver ulike lovpålagte internkontrollplikter i separate systemer, eller om de samler to eller flere slike plikter til et felles system. Disse momentene, som begge kan begrunne en plikt til å dokumentere organiseringen, synliggjør noen av de valg og beslutninger den enkelte virksomhet treffer innenfor sitt handlingsrom. Å treffe beslutning om hvordan virksomheten organiserer internkontrollarbeidet kan betraktes som en side av aktivitetsplikten. Handlingsrommet er stort, men fravær av aktive valg og beslutninger vil være et pliktbrudd.

4.3.1.1 Noen typer unntak, der det er lagt rettslige føringer for organiseringen

I utgangspunktet står altså en virksomhet fritt til å velge sin organisering av internkontrollsystemet. De generelle begrensningene i denne friheten, som man sjelden finner eksplisitt uttrykt, må ligge i at organiseringen skal være effektiv nok til at oppgavene blir utført, og til at systemet er etterprøvbart.

Det finnes enkelte unntak, der rettsregler legger føringer for organiseringen. Slike føringer innebærer prinsipielt en innskrenkning i virksomhetenes suverenitet. I denne sammenheng er det bare føringer for organiseringen av internkontrollsystemet som er av interesse. Det finnes også andre rettslige pålegg om organisering, som ikke henger sammen med en plikt til internkontroll.[190] For å regne noe som føringer for organiseringen av internkontrollsystemet, må det enten være knyttet direkte til en internkontrollplikt, eller være klart begrunnet i behovet for å sikre et samfunnshensyn som er underlagt krav om internkontroll. Man kan klassifisere slike føringer etter hvilket formål de skal tjene. Det synes å forekomme tre ulike, men ikke skarpt avgrensede, formål.

Det første formålet er å sikre den vertikale integriteten i internkontrollarbeidet, slik at samfunnshensynet ikke svekkes dersom deler av virksomheten er utkontraktert eller delegert til underordnete organer. [191] Andre varianter av regulering som sikrer vertikal integritet kan ha mer indirekte karakter. Databehandleravtaler er en reguleringsmekanisme for å sikre personopplysninger, enten ved utkontraktering eller dersom de på annet vis reelt håndteres andre steder enn innenfor den ansvarliges virksomhet.[192]

Det andre formålet er å sikre tilstrekkelig tyngde og gjennomslag for virksomhetsinterne kontrollfunksjoner. Et virkemiddel for å sikre dette, er å fastsette regler om uavhengighet.[193] Et annet virkemiddel er å gi regler om sammensetningen av en intern kontrollfunksjon. I stedet for uavhengighet fra daglig ledelse, innebærer slike krav til sammensetning normalt at både ledelsen og andre berørte har felles ansvar for kontrollen. Et eksempel er plikten til å

[190] Et eksempel er hovedregelen om organisering av offentlige organers arkivtjeneste, som ikke er knyttet til internkontroll: «Arkivarbeidet i eit offentleg organ skal som hovudregel utførast av ei eiga eining, ei arkivteneste, under dagleg leiing av ein arkivansvarleg.» arkivforskrifta, 11. desember 1998 nr. 1193 § 2-1 første punktum.

[191] Et eksempel på en sterk variant av formålet vertikal integritet finnes i petroleumsloven. Rettighetshaver har plikt til *å påse*: «I tillegg plikter rettighetshaver å påse at enhver som utfører arbeid for seg, enten personlig, ved ansatte eller ved entreprenører eller underentreprenører, overholder bestemmelsene gitt i eller i medhold av loven.» petroleumsloven [1996] § 10-6 annet punktum.

[192] Bestemmelsene er omtrent likelydende i helseregisterloven og personopplysningsloven. Sitert fra helseregisterloven § 18: «En databehandler kan ikke behandle helseopplysninger på annen måte enn det som er skriftlig avtalt med den databehandlingsansvarlige. Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse. I avtalen med den databehandlingsansvarlige skal det også gå frem at databehandleren plikter å gjennomføre slike sikringstiltak som følger av § 16.»

[193] Krav til en uavhengig kontrollenhet innenfor virksomheten finner man i forskriftsbestemmelser om internrevisjon i finansinstitusjoner, men det er ellers lite utbredt. Internrevisjonens uavhengighet fra den daglige ledelse er ivaretatt gjennom at internrevisjonens leder tilsettes og avskjediges av styret, og har rett til å møte i styremøtene. Disse kravene ble først forskriftsfestet i internkontrollforskrift finansinstitusjoner, 20. juni 1997 nr. 1057, (Opphevet). Forskriften er erstattet av en ny forskrift som viderefører samme ordning, forskrift om risikostyring og internkontroll, 22. september 2008 nr. 1080. Et mildere krav til uavhengighet, en bekreftelse av den interne kontroll fra en «instans utenom den operative organisasjonen», fantes i to tidligere forskrifter, for henholdsvis banker og forsikringsselskaper.

etablere kvalitetsutvalg i sykehusene.[194] Hjemmelen til å gi forskrifter om kvalitetsutvalg er ikke brukt, men en retningslinje som fremdeles gjelder ble gitt som vedlegg til et rundskriv i 1994.[195] Kvalitetsutvalgenes oppgaver og myndighet har vært et gjennomgående tema i Helsetilsynet systemrevisjoner overfor helseinstitusjoner.

Den tredje formen for begrensninger i virksomheters frihet til selv å velge organisering av internkontrollsystemet er å pålegge virksomheten å ha et tydelig og synlig kontaktpunkt for sitt arbeid med å ivareta det aktuelle samfunnshensynet. Kontaktpunktets primære funksjon vil som regel være å koordinere samhandlingen mellom virksomheten og et statlig tilsynsorgan, men det kan også dreie seg om kontakten med eiere, overordnet organ, brukere eller allmennheten.[196] Også på visse andre områder forekommer pålegg om å utpeke enkeltpersoner som kontaktpunkt eller til å ha ansvar for bestemte oppgaver. Ofte er dette hovedsakelig et tiltak for å sikre tilstrekkelige fagkunnskaper.[197] Generelt har lovgiver vært tilbakeholdende med å lovfeste slike funksjoner. En personlig fullmakt innenfor en virksomhet vil kunne oppfattes som en «stat i staten», og innebære en begrensning i virksomhetenes handlingsrom. «Strålevernsansvarlige» er et eksempel på utpekte kontaktpersoner med fullmakter som innebærer en viss grad av uavhengighet av virksomhetsledelsen. Virksomheter som anvender eller installerer ioniserende strålekilder skal utpeke en eller flere stråle-

[194] Kvalitetsutvalgene ble innført i den tidligere sykehusloven, sykehusloven, 19. juni 1969 nr. 57, (Opphevet) § 18b, samtidig med at internkontroll som tilsynsmetode ble innført generelt for helseinstitusjoner, i 1992. Ordningen er videreført i den nåværende spesialisthelsetjenesteloven, 2. juli 1999 nr. 61 § 3-4: Kvalitetsutvalg skal opprettes «som ledd i den internkontroll institusjonen er pliktig til å føre i henhold til § 3 i lov 30. mars 1984 nr. 15 om statlig tilsyn med helsetjenesten.»

[195] Rundskrivet var altså gitt i medhold av den daværende sykehusloven. I retningslinjen anbefales det at kvalitetsutvalg opprettes med noen faste medlemmer; en representant fra ledelsen, en representant fra de medisinsk-tekniske tjenester, verneombudet og en brukerrepresentant. Helsetilsynet ser brukerrepresentasjon som «ett av flere virkemidler i det generelle arbeid med å styrke brukermedvirkningen og rettssikkerheten for pasienter i helsetjenesten.» *Retningslinjer for kvalitetsutvalgenes oppgaver, funksjon og sammensetning* (1994).

[196] Et eksempel finnes i Sprengstoffinspeksjons retningslinje fra 1982: «Bedriften skal utpeke en kontaktperson overfor Sprengstoffinspeksjonen. Kontaktpersonen bør fortrinnsvis også administrere internkontrollen.» internkontrollforskrift brannfarlig vare punkt 5(6).

[197] For eksempel: «Hver biobank skal ha en ansvarshavende person med medisinsk eller biologisk utdannelse av høyere grad.» behandlingsbiobankloven, 21. februar 2003 nr. 12 § 7 første punktum. Den ansvarshavende utpekes av den som er databehandlingsansvarlig. Det dreier seg derfor om mer eller mindre ordinær delegasjon, men virksomheten kan altså ikke velge bort det å utpeke en ansvarlig person. Den utpekte ansvarshavende skal «sørge for at biobanken opprettes og forvaltes i samsvar med denne og annen lov.»

vernsansvarlige.[198] Også i EU-regelverk finner man krav til at virksomheter utpeker enkeltpersoner med spesielt ansvar.[199]

Kontaktperson for et samfunnshensyn kan også være en ordning som er frivillig for virksomhetene. I personverndirektivets bestemmelser om behandlingsansvarliges meldeplikt til tilsynsmyndigheten, er det en åpning for å gjøre unntak fra meldeplikten blant annet «når den behandlingsansvarlige i samsvar med den nasjonale lovgivning vedkommende er underlagt, utpeker en person med ansvar for beskyttelse av personopplysninger», og denne personen har visse nærmere angitte oppgaver.[200] I Norge er dette implementert under betegnelsen personvernombud. Virksomheter kan ikke pålegges å utnevne personvernombud, men Datatilsynet kan samtykke i unntak fra meldeplikten, dersom virksomheten utnevner et personvernombud som er uavhengig.[201] Personvernombudet får formelt sett alle sine fullmakter fra arbeidsgiveren. Det er derfor noe uklart hva uavhengigheten egentlig består i. I Datatilsynets veiledningsdokument er det å bistå den registrerte, ved forespørsler om innsyn eller korrigering, blant de oppgavene de anbefaler å legge til personvernombudet. Et internt ombud som er uavhengig av virksomhetens ledelse vil kunne være problematisk og uryddig i kontakten med enkeltpersoner utenfor virksomheten. Det er mer nærliggende å forstå uavhengigheten etter forskriftsbestemmelsen dit hen at det er en viss uavhengighet i funksjonen som kontaktperson overfor Datatilsynet.[202]

Helsepersonelloven inneholder også enkelte eksempler på at særskilte kompetanser legges til bestemte personer, i stedet for at virksomheten stilles fritt. Dette er omtalt, med

---

[198] «Ved særlig omfattende bruk av ioniserende stråling må den strålevernsansvarlige kunne utføre eller få utført fysiske, tekniske og radiokjemiske målinger og vurderinger for å bestemme stråledoser, og må også kunne vurdere helserisiko og konsekvenser ved forskjellige uhellsituasjoner som kan oppstå», strålevernforskriften, 21. november 2003 nr. 1362 § 8(3). I Helse- og omsorgsdepartementets merknader til de enkelte paragrafer, publisert sammen med forskriften i Norsk Lovtidend avdeling I, 2003, s. 2481, tilføyes en forutsetning som ikke fremgår av forskriftsteksten: «Strålevernansvarlig skal også være en kontaktperson som tilsynsmyndigheten kan forholde seg til.»

[199] I direktiv om standarder for kvalitet og sikkerhet ved håndtering av humane vev og celler, kreves det at alle «vævscentre udpeger en ansvarlig person, som skal opfylde følgende minimumskrav og kvalifikationer.» En av oppgavene som tilligger den ansvarlige person er «at oplysninger indsendes til den eller de ansvarlige myndigheder i henhold til kravene i artikel 6.» EP/Rdir 2004/23/EF artikkel 17(2)(b). I norsk implementering av direktivet kreves det at virksomheten utnevner ansvarlig person med visse kvalifikasjoner, ansvar for at bestemte oppgaver utføres i samsvar med gjeldende regelverk, og at virksomheten underretter Helsedirektoratet om navnet på den ansvarlige personen, forskrift om humane celler og vev, 7. mars 2008 nr. 222 § 6.

[200] EP/Rdir 95/46/EF artikkel 18(2).

[201] «Datatilsynet kan samtykke i at det gjøres unntak fra meldeplikt etter personopplysningsloven § 31 første ledd, dersom den behandlingsansvarlige utpeker et uavhengig personvernombud som har i oppgave å sikre at den behandlingsansvarlige følger personopplysningsloven med forskrift. Personvernombudet skal også føre en oversikt over opplysningene som nevnt i personopplysningsloven § 32.» personopplysningsforskriften § 7-12.

[202] Det fremgår av Datatilsynets veiledningsdokument på området at Datatilsynet stiller noe mer detaljerte krav til et personvernombuds fullmakter enn det som fremgår av forskriftsteksten, som vilkår for å samtykke i unntak fra meldeplikten. Et av disse vilkårene er «å gi Datatilsynet opplysninger dersom tilsynet ber om det, herunder foreta undersøkelser i konkrete saker.» *Personvernombud. Ombudets rolle og arbeidsoppgaver.* (2007), s. 5.

henvisning, i kapittel 3.5 i sammenheng med enkelte faglige prerogativer for profesjonsutøvere.

4.3.1.2 Medbestemmelsesrett og medvirkningsplikt

Både rettslig og ideologisk forutsetter internkontroll at virksomheten involverer de ansatte i prosessen. Internkontrollutvalget skisserte tre grunner til at arbeidstakerne bør ha medinnflytelse:

> For det første utgjør arbeidstakerne en vesentlig ressurs, i det det er disse som har de daglige erfaringer med virksomheten. … For det annet er medinnflytelse viktig i seg selv som en arbeidsmiljøfaktor. Endelig vil medinnflytelse skape større sikkerhet for at de rutiner som blir etablert faktisk også blir etterlevet.[203]

Begrunnelse nummer to i sitatet ovenfor dreier seg om medbestemmelse som en rettighet. Medbestemmelsesrett kommer stort sett bare til uttrykk i internkontrollbestemmelser der samfunnshensynet er arbeidstakervern.[204] Internkontroll er også knyttet til medbestemmelsesapparatet, ved at det inngår både i verneombudets og arbeidsmiljøutvalgets oppgaver.[205] Medbestemmelse som rettighet er imidlertid mindre relevant for andre kategorier av samfunnshensyn enn arbeidstakervern. Dersom samfunnshensynet er personvernet til virksomhetens pasienter eller kunder, eller kvaliteten på fremtidige generasjoners drikkevann, har ikke arbeidstakere særskilte interesser å gjøre gjeldende. Like fullt er de ansattes medvirkning vektlagt både i forskrifter og veiledninger om internkontroll. Dette må da henge nærmere sammen med de to andre begrunnelse som internkontrollutvalget skisserte: De ansatte som kunnskapskilde ved utarbeidelsen, og deres forståelse for, eller lojalitet til, rutinene som skal etterleves. Dermed handler ikke arbeidstakerens deltakelse bare om medbestemmelse og bedriftsdemokrati. Arbeidstaker har også en medvirkningsplikt.[206]

Plikter til å medvirke finner man også i internkontrollbestemmelser som gjelder andre samfunnshensyn enn arbeidstakervern. En formulering som forekommer i lik eller nesten lik ordlyd i flere forskrifter om internkontroll er denne: «[Internkontroll innebærer at den/de

[203] NOU 1987:10, s. 43.
[204] Slike rettigheter var til stede i lovgivningen allerede før internkontroll ble innført, ettersom internkontrollsystemer måtte anses å være omfattet av retten til å «holdes orientert om systemer som nyttes ved planlegging og gjennomføring av arbeidet, herunder om planlagte endringer i slike systemer. … og de skal være med på å utforme dem.» arbeidsmiljøloven [1977] § 12 nr. 3.
[205] For verneombudets del er dette utformet slik i nåværende lov: «Verneombudet skal tas med på råd under planlegging og gjennomføring av tiltak som har betydning for arbeidsmiljøet innenfor ombudets verneområde, herunder etablering, utøvelse og vedlikehold av virksomhetens systematiske helse-, miljø- og sikkerhetsarbeid, jf. § 3-1.», arbeidsmiljøloven [2005] § 6-2 nr. 4.
[206] «Arbeidstaker skal medvirke ved utforming, gjennomføring og oppfølging av virksomhetens systematiske helse-, miljø- og sikkerhetsarbeid.» Arbeidsmiljøloven [2005] § 2-3 nr. 1 første punktum.

ansvarlige for virksomheten skal:] sørge for at arbeidstakerne medvirker slik at samlet kunnskap og erfaring utnyttes.»[207] Etter ordlyden er det altså virksomheten, ved dens ledelse, som pålegges å utnytte de ansattes kunnskaper, dog ikke nødvendigvis som eneste kunnskapskilde. Arbeidstakers plikt til å medvirke følger av arbeidsplikten.

Et annet eksempel illustrerer den tredje begrunnelsen, de ansattes forståelse for og lojalitet til rutinene. Også dette er en plikt for virksomheten, som samtidig impliserer en plikt for arbeidstakeren. «[Internkontroll innebærer at virksomheten skal:] sørge for at arbeidstakerne har tilstrekkelige og oppdaterte kunnskaper og ferdigheter i virksomhetens internkontroll.»[208]

Veiledningsmateriell fra tilsynsorganer viser av og til at medvirkningens formål og grunnlag ikke nødvendigvis tas så nøye. Det er kanskje snarere en «målet helliger midlet»-tankegang, i stedet for å ta stilling til om medvirkning skal være en plikt eller rettighet, og hvem som i så fall er forpliktet eller berettiget, er det medvirkning som middel for å bedre kvaliteten i internkontrollsystemet som er vektlagt. Dette eksemplet er et utdrag fra en veileder om internkontroll i barnevernstjenesten:

> Internkontroll er avhengig av at medarbeidere deltar med sin kunnskap og erfaring i arbeidet med kartlegging, planlegging og med å finne gode løsninger. Dette kan gjøres gjennom egne arbeidsgrupper, allmøter, samarbeid med tillitsvalgte eller på andre hensiktsmessige måter. Slik sikrer man også ansvarliggjøring og medvirkning fra medarbeiderne. Dette er helt avgjørende for at internkontrollen skal fungere som forutsatt.[209]

Veilederen tar utgangspunkt i forskriftens begrunnelse for medarbeidernes deltakelse, men gir upresise anvisninger på hvordan medvirkningen skal foregå. Ikke alle måtene å medvirke på kan sies å følge av arbeidsplikten, veilederen blander sammen elementer av medbestemmelsesrett og medvirkningsplikt. Etatens hovedanliggende er neppe å tydeliggjøre det rettslige grunnlaget, men at veiledningen skal gi gode internkontrollsystemer som resultat.

4.3.2 Beslutninger om mål og kriterier for aksept av risiko

Selve samfunnshensynet som ligger bak en bestemt plikt til internkontroll befinner seg egentlig på utsiden av idealtypen. Det metodetrinnet som er kalt «beslutninger om mål og kriterier for aksept av risiko» er et krav til å *internalisere* samfunnshensynet. Virksomheten skal gjennomføre de aktiviteter som er nødvendige for å operasjonalisere de bestemmelsene i

[207] Internkontrollforskrift i sosial/helsetjenesten, 20. desember 2002 nr. 1731 § 4(2)(d).
[208] Forskrift om IK-Akvakultur, 19. mars 2004 nr. 537 § 5(2)(2).
[209] *Internkontroll i barneverntjenesten i kommunene – en veileder.* (2006), s. 5.

lov eller forskrift, eller den rettslige standarden, som internkontrollplikten henviser til. Virksomhetens egne fastsatte mål, på det området internkontrollsystemet dekker, er en beslutning som skal dokumenteres og som virksomheten må kunne innestå for.[210]

Det risikoproblemet som oppstår i de ulike kategoriene samfunnshensyn som er beskrevet her kan betegnes som en regulering av risikoskapers virksomhet, der risikobæreren normalt ikke er representert eller direkte berørt.[211] Internkontroll er, etter idealtypen, risikoskaperens selvregulering. Risikobærerens behov og interesser ligger i samfunnshensynet, og er en del av det som risikoskaperen skal internalisere. Det er imidlertid risikoskaperen som har både aktivitetsplikten og initiativretten. Risikobæreren, enten det er en enkeltperson eller en kollektiv entitet, blir i større grad en interessent med demokratiske handlingsalternativer enn en rettighetshaver. Når en virksomhet selv har definert hva de anser som akseptabel risiko, og dette ikke overprøves av kompetente myndigheter, er det lite grunnlag for kritikk mot virksomheten når feil og avvik innenfor det aksepterte inntreffer. En allmenn aksept for den feiltoleransen som ligger innebygd i idealtypisk internkontroll kan imidlertid være vanskelig å oppnå på områder der tilliten hos den enkelte risikobærer er viktig. Denne problemstillingen er gjenstand for omfattende drøfting innen risikobasert regulering i helsesektoren.[212]

Beslutninger om mål og aksept av risiko i et internkontrollsystem er mer enn bare valg av feiltoleranse. Det er også et grunnleggende valg av strategi for håndtering av risiko. Aaron Wildavsky introduserte to universelle, man kan kalle dem idealtypiske, strategier for risiko-håndtering.[213] Å foregripe betyr at man søker å unngå feil og avvik, mens resiliens er å utbedre skader, lære, og tilpasse seg til det som forvolder skaden. Disse to universelle strategiene vil finnes i ulike blandingsforhold i alle slags systemer som er gjenstand for risiko. Et resonnement som Wildavsky setter av mye plass til, og eksemplifiserer med ulike typer systemer, er at resiliensstrategier i mange tilfeller gir et tryggere samfunn enn forsiktighets-

[210] Som metodetrinn i idealtypen dreier «aksept av risiko» seg om å fastlegge virksomhetens egen toleranse for feil og avvik. Dette skiller seg fra måten begrepet brukes på i den erstatningsrettslige læren om aksept av risiko, der det betyr at den skadelidte har akseptert å bære risikoen slik at grunnlaget for erstatning faller bort. Begrepet er brukt slik for eksempel i *røykedommen*. Etter at helseskadene ved røyking må ha vært allment kjent, Høyesterett fastsatte årstallet til 1964, var det å røyke noe man gjorde for egen risiko, jf. Rt. 2003 s. 1546.

[211] Forholdet mellom risikoskaper og risikobærer er blant annet drøftet i en bredt anlagt artikkel, primært med eksempler fra naturressurs- og miljøregulering, som en fundamental forskjell mellom ulike reguleringstradisjoner som det er vanskelig å forene. Christopher H. Schroeder (1986): «Rights against Risks». I: *Columbia Law Review,* s. 495–562.

[212] Sally M. Lloyd-Bostock og Bridget M. Hutter (2008): «Reforming regulation of the medical profession: The risks of risk-based approaches». I: *Health, Risk & Society,* s. 69–83.

[213] «Anticipation» (i betydningen å forvente eller foregripe), og «resilience», er nøkkelbegreper som utvikles i Aaron Wildavsky (1988): *Searching for safety*.

strategier. Det har vært bemerket at risikobasert internkontroll er en direkte motsats til det populære begrepet «nulltoleranse».[214]

Det idealtypiske internkontrollsystem forutsetter også en kombinasjon av foregripelse og resiliens. Metodetrinnet *risikoreduserende tiltak* er en strategi for å foregripe, mens *håndtering av avvik* er en resiliensstrategi. En virksomhet kan neppe sies å ha et gangbart internkontrollsystem dersom ikke begge disse elementene er på plass. Vektleggingen mellom foregripelse og resiliens er en strategisk beslutning, som virksomheten uttrykker gjennom sine mål og sin aksept av risiko.

Retten til å beslutte mål og aksept av risiko er et sterkt uttrykk for virksomhetens handlingsrom. Den har imidlertid også sine grenser. Vage og standardpregete angivelser av et samfunnshensyn skal ikke strekkes for langt, oppfyllelsen må baseres på holdbar tolkning og operasjonalisering. I noen tilfeller gir regelverket føringer for hva som er akseptabel risiko, det forekommer også at tilsynsorganer har adgang til å overprøve virksomhetens beslutninger. På den annen side er handlingsrommet i et idealtypisk internkontrollsystem større, og av en annen karakter, enn bare en forventning om at hver virksomhet skal lykkes i å treffe med beslutninger som er «objektivt riktige» i den betydning at andre med samme innsikter og ferdigheter ville ha kommet frem til samme beslutning. Idealtypens posisjon er at virksomheten har rett til å veie egeninteresser mot ulike samfunnshensyn, slik at myndighetsinngrep krever at forsømmelsene av et samfunnshensyn overstiger en viss terskel.

4.3.3 Risikovurderinger

Et høyt antall forskrifter inneholder en plikt til å vurdere, eller analysere, risiko. Denne plikten er ofte, men ikke alltid, innkapslet i plikten til å utøve internkontroll.[215] En risikovurdering er en aktivitet som skal systematisere, og eventuelt generere, kunnskaper om risiko. Det finnes flere forskjellige metoder for risikovurderinger, men metodene inneholder stort sett de samme grunnleggende elementene. Vurderingsmetoden som velges er prinsipielt uavhengig av hvilket samfunnshensyn som reguleres. I forordet til Norsk standard for risikovurderinger, som er et velegnet og velkjent uttrykk for de generelle trekkene ved metodikken, er gyldighetsområdet beskrevet så åpent som dette: «Standarden er relatert til alle typer risikovurderinger, bortsett fra vurdering av økonomisk risiko som følge av forretningsmessige

[214] «Political discourses of 'zero-tolerance' sit uneasily with a risk-based ethos.» Power (2004), s. 22.
[215] Et eksempel på bruk av formelle metoder, der risikovurdering ikke er direkte knyttet til internkontroll, er skjema for å vurdere voldsrisikoen i psykisk helsevern. *Vurdering av risiko for voldelig atferd: bruk av strukturerte kliniske verktøy.* (2007).

disposisjoner.»[216] Risiko er formelt definert i standarden som «uttrykk for kombinasjonen av sannsynligheten for og konsekvensen av en uønsket hendelse.» Begrepene sannsynlighet, konsekvens og uønsket hendelse er igjen definerte begreper i standarden. «Uønsket hendelse» er definert som «en hendelse som kan medføre tap av verdier», en definisjon som åpner for et nærmest bemerkelsesverdig stort spenn av verdibedømmelser.

Tilsynsorganers veiledningsdokumenter har en tendens til å nedtone omfanget – men ikke viktigheten – av risikovurderinger. Veiledningsdokumentene er ofte ute i et slags avdramatiseringsærend.[217] Barne- og likestillingsdepartementets veileder for internkontroll i barneverntjenesten stiller opp tre punkter for risikoanalyse. De vektlegger også at det skal være enkelt, og toner ned den formelle metodikken.

> En enkel risikoanalyse kan være å stille tre enkle spørsmål:
> - Hvilke faktorer kan medføre at vi ikke innfrir målene?
> - Hva kan vi gjøre for å redusere sannsynligheten for at dette skjer?
> - Er det noe vi kan gjøre for å redusere konsekvensene dersom dette skjer?[218]

Igjen er antakelig det som ligger bak et behov for å unngå at den enkelte virksomhet skal oppleve terskelen som høy. Å svare på disse tre «enkle» spørsmålene er imidlertid det som i realiteten er vanskelig å få til, uansett hvilke verktøy og formelle eller uformelle metoder man velger å benytte. Problemet ligger i å finne frem til hvilke faktorer som utgjør risiko.[219]

Selv de mest formelle og stringente standarder og veiledninger blir litt omtrentlige i spørsmålet om hvordan man identifiserer hvilke hendelser som er uønskede, og som dermed skal underlegges vurdering. Metodene for å identifisere risikofaktorer dreier seg om å bygge på erfaring, faglige basiskunnskaper og normer, gjerne i kombinasjon med å utarbeide mer konkrete scenarioer. Standarden bygger godt opp under metodeverktøyene som virkemidler for å sikre at risikovurderingene blir objektive og etterrettelige. Slik sett kan risikovurderinger minne om forskning, den langsiktige troverdigheten og påliteligheten er basert på åpenhet om, og kontinuerlig kritikk av, både metoder og resultater. I en sosialantropologisk studie av risikohåndtering fant Mary Douglas at de som arbeider med risikovurderinger er opptatt av å presentere risikovurderingene som vitenskapelige og nøytrale, til tross for at hver enkelts

[216] NS 5814:2008. «Krav til risikovurderinger». Dette er andre utgave av standarden, første utgave kom i 1991.
[217] Et eksempel, fra veiledning til internkontrollforskriften for sosial- og helsetjenesten: «Dette kan gjøres enkelt ved at det f eks organiseres som en idédugnad, men om ønskelig finnes det mer avansert analyseverktøy for risikovurdering.» *Hvordan holde orden i eget hus: Internkontroll i sosial- og helsetjenesten*, s. 29.
[218] *Internkontroll i barneverntjenesten i kommunene – en veileder*, s. 10.
[219] I standardens formelle metodikk kalles denne delen av analysen «identifikasjon av farer og uønskede hendelser». NS 5814:2008.

vurderinger viste seg å være sterkt farget av vedkommendes verdier og faglige og politiske ståsted.[220]

I en viss forstand ligger det et paradoks i ønsket om at risikovurderingen skal fremstå som nøytral og objektiv. Identifiseringen av hvilke uønskede hendelser man skal vurdere, og selve vurderingen, er det metodetrinnet i internkontrollen hvor virksomheten har størst grad av reelle muligheter til å påvirke resultatet. Dermed kunne valg og prioriteringer i risikovurderingsaktivitetene være godt egnet som arena for å dreie internkontrollen i retning av virksomhetens egeninteresser. I arbeidet med å identifisere risikofaktorer, ta stilling til sannsynligheten for at de inntreffer, og konsekvensene hvis eller når det skjer, er risikoskaperens definisjonsmakt nærmest ubegrenset. Eksterne tilsynsorganer kan, i varierende grad ut fra detaljer i regelverket og etablert praksis, overprøve både aksept av risiko og hvor egnet de valgte risikoreduserende tiltakene er. Vurderingene som ligger bak har de derimot liten innflytelse over. Likevel er det grunn til å tro at virksomhetene, i den grad de gjennomfører og lykkes med sine risikovurderinger, etterstreber en troverdig fremstilling av risikofaktorene. Risikovurderingene er mer enn en etappe i et kontrollopplegg, de har en egenverdi. Det er først og fremst i denne aktiviteten at kunnskaper om kontrollbehovet, og om evnen til å ivareta samfunnshensynet, blir generert og kommunisert, både internt i virksomheten, til eiere eller overordnede organer, og til eksterne tilsynsorganer.

Når man tar i betraktning det høye antallet plikter til internkontroll i lov og forskrift, der en viktig premiss for pliktens omfang og innhold er virksomhetens egen identifikasjon og vurdering av risikofaktorer, er det relativt lite akademisk kritikk av risikovurderingenes egnethet og treffsikkerhet som metode. Den tendensen til å tone ned de formelle metodene som man kan finne i noen av tilsynsorganenes veiledninger setter kanskje indirekte et spørsmålstegn ved egnetheten. Virksomhetene trenger et velutviklet begrepsapparat, og erfaringer med metoden, i tillegg til de fagkunnskapene som inngår i vurderingene. Derfor kan det være ressurskrevende og byrdefullt å utarbeide en pålitelig og veldokumentert risikovurdering, særlig for små virksomheter.

I Storbritannia har flere forskere inntatt en mer kritisk holdning til internkontroll, risikobasert regulering og andre beslektede former for «lighter-touch regulations». Et problem, som drøftes i forskning på britisk helseregulering, er om risikobasert regulering kan eller bør ta hensyn til opinionen og offentlighetens «risikoappetitt».[221] Hvilke elementer som skal legges til grunn i risikobasert regulering er et politisk spørsmål. Hvis risikoorienteringen

[220] Mary Douglas (1992): *Risk and Blame: Essays in Cultural Theory*.
[221] Lloyd-Bostock og Hutter (2008).

fagliggjør politiske spørsmål, blir grunnlaget for beslutningenes legitimitet snevrere. Dette problemet kommer særlig på spissen der samfunnshensynet er innen kategorien forsvarlighet, rettssikkerhet og individers rettighetsvern. Et annet problem er den interessante dreiningen som Michael Power påviser og advarer mot: Virksomheters ledelse flytter over tid oppmerksomheten fra det han betegner som førsteordens risiko til sekundær risiko.[222] Førsteordens risiko er uønskede hendelser og negative konsekvenser av direkte betydning for det aktuelle samfunnshensynet. Sekundær risiko er trusselen om sanksjoner eller negative konsekvenser for virksomhetenes omdømme, eller til og med konsekvenser for ledernes personlige renommé, uttelling i et belønningssystem eller videre karrieremuligheter.

Et mulig eksempel på omformulering av en hendelses negative konsekvenser, fra primær til sekundær risiko, kan være fra «kunden taper penger» til «bankens omdømme svekkes». Dette er ikke nødvendigvis en avdramatisering av konsekvensen. Tvert i mot kan bankens ledelse bli mer skremt av tanken på svekket omdømme, og etterfølgende langsiktige tap, enn av å utsette enkeltkunder for urett eller ubehag. Ut fra en ren kvantitativ risikovurdering, kan det koste mindre å erstatte noen kunders tapte penger enn å investere i egnede risikoreduserende tiltak. En risikovurdering som omfatter omdømmekonsekvenser kan rette opp denne skjevheten i regnestykket, slik at de risikoreduserende tiltakene likevel lønner seg. I dette enkle, konstruerte eksemplet bidrar altså oppmerksomhet om en sekundær risiko til bedre konkret risikohåndtering. Det er også i tråd med noe av ideologien bak et risikobasert internkontrollsystem; å ivareta samfunnshensynene bør så langt det er mulig spille på lag med virksomhetens egeninteresser.[223] Man har imidlertid ingen garanti for at opptattheten av sekundær risiko alltid vil forsterke virksomhetens opplevelse av behovet for å ivareta samfunnshensynet. For å trekke eksemplet litt videre, kan den samme banken ha kommet til at det er mer lønnsomt å investere direkte i polering av omdømmet enn å investere i risikoreduserende tiltak. Den enkelte kunde løper fortsatt samme risiko for å tape penger, men dersom omdømmestrategien lykkes vil det være færre som klandrer banken for det.

Både problemet med fagliggjort kamuflering av politiske spørsmål og problemet med å bli opptatt av sekundær risiko peker på et sårbart punkt ved risikobasert internkontroll som reguleringsmetode: Risikovurderinger anviser ikke entydige sammenhenger mellom hver risikofaktor og tiltakene for å håndtere eller redusere risikoen. Samme hendelse har ofte flere lag av konsekvenser. Selv om tiltak for å håndtere førsteordens risikoer er mest transparente og etterprøvbare fra et regulatorisk synspunkt, kan det likevel være mer nærliggende for en

[222] Power (2004).
[223] Jf. omtalen av COSO-rapporten i kapittel 4.2.1 ovenfor.

virksomhet å velge tiltak rettet mot sekundær risiko. Sammenhengen mellom det aktuelle samfunnshensynet og en sekundær risiko for virksomheten er nødvendigvis obskurt.

Flere veiledninger om internkontroll legger vekt på å fremstille risikovurdering så enkelt som mulig, og nøyer seg med å nevne at mer formelle metoder kan brukes. Datatilsynet har også en enkel beskrivelse av risikovurderinger som del av en generell veiledning om internkontroll i mindre virksomheter. I tillegg har de gitt ut et eget mer omfattende og sikkerhetsfaglig metodeforankret veiledningsdokument. I den mer omfattende veilederen trekker de inn forhold som gjelder risikostyring som egen metodisk disiplin. Veilederen oppfordrer til at risikovurderingene blant annet baseres på den verdi informasjonen har som aktivum for organisasjonen. I nærmere forklaring av de verdiene som skal identifiseres nevnes også sekundær risiko, «indirekte kostnader som tap av 'goodwill' osv.»[224] Både informasjonen som aktivum og tap av goodwill beveger seg utenfor en snever avgrensning av informasjonssikkerhet for å ivareta den enkelte registrertes personvern. Med denne mer metodebaserte veiledningen åpner Datatilsynet for å identifisere et bredt omfang av risikofaktorer, noe som gjør sammenhengen mellom risikovurderingen og det samfunnshensynet Datatilsynet er ansvarlig for mindre tydelig.

4.3.4 Risikoreduserende tiltak

Neste idealtypiske metodetrinn er strategiske beslutninger om egnede tiltak, eller virkemidler, for å nå de målene virksomheten har besluttet. Et grunnleggende krav som stilles til tiltakene er at de skal være planlagte og systematiske. Planlagt og systematisk står her i motsetning til sporadiske eller rent situasjonsbetingede tiltak. Både valg av tiltak og gjennomføringen av tiltakene skal dokumenteres i tilstrekkelig grad til å kunne etterprøves av en ekstern instans. Hensikten er å foregripe uønskede hendelser i rimelig grad. Lov eller forskrift gir ofte noen føringer, som ikke er uttømmende, for hva tiltakene bør gå ut på. Det kan være generelle tiltak som opplæring av ansatte, eller mer spesifikke tekniske tiltak tilpasset det enkelte fagområde, som for eksempel temperatur for oppbevaring av matvarer eller regler om sikkerhetskopiering av data.

Strålevernforskriften gir anvisninger på flere ulike tiltak, som skal iverksettes dersom risikovurderingen viser «at det finnes en risiko for ansatte, andre personer eller miljø, eller at strålekilder kan komme på avveie.»[225] De tiltakene det gis anvisning på er ikke særlig konkret

[224] *Risikovurdering av informasjonssystem med utgangspunkt i forskrift til personopplysningsloven.* (2002), s. 9.
[225] Jf. strålevernforskriften § 9.

utformet. Virksomheten skal «[f]oreta alle rimelige praktiske tiltak for å unngå eller redusere sannsynligheten for slike hendelser», sikre radioaktive kilder mot tyveri og skadeverk, planlegge tiltak for å redusere konsekvensene av slike hendelser etc.[226] Virksomheten står fritt til å velge hvilke tiltak de anser som gode nok innenfor disse rammene. Fravær av tiltak som er relevante for de ulike punktene i forskriftens § 9 vil imidlertid måtte anses som et pliktbrudd.

En enda mer generell utforming har kravet til å gjennomføre risikoreduserende tiltak etter forskrift om smittevern i helsetjenesten: «Programmet skal også omfatte tiltak for å verne ansatte mot smitte.»[227]

På enkelte områder gir forskriftene mer konkrete føringer for de risikoreduserende tiltakene. Støyforskriften gjelder etter sin § 2 generelt «for virksomheter der arbeidstakere kan bli utsatt for støy i forbindelse med arbeidet.» Forskriftens § 10 pålegger risikoreduserende tiltak: «Arbeidsgiveren skal iverksette nødvendige tiltak på bakgrunn av de helse- og sikkerhetsrisikoer som fremkommer av risikovurderingen.» De første føringene for tiltakene er relativt åpne, som å vurdere alternative arbeidsmetoder og velge hensiktsmessig arbeidsutstyr. Lenger ned i listen (§ 10 bokstav d) anvises teknisk støyreduksjon, med *eksempler* på konkrete tiltak for dette, skjermer, innbygging eller lydabsorbenter. Tiltaket å «tilrettelegge arbeidet ved begrensning av eksponeringstid og intensitet, og med tilstrekkelige støyfrie hvileperioder» (§ 10 bokstav g) etterlater lite valgfrihet for arbeidsgiveren.[228] Støyforskriften er norsk implementering av EUs støyverndirektiv.[229]

En annen variant av føringer for risikoreduserende tiltak er prinsippene for risikoreduksjon i internkontrollforskriftene for petroleumsvirksomheten. Rammeforskriften om helse, miljø og sikkerhet i petroleumsvirksomheten anviser generelle avveiningsnormer, blant annet om hvilken usikkerhet det vil være viktigst å redusere først ved en eventuell motstrid:

> Ved reduksjon av risiko skal den ansvarlige velge de tekniske, operasjonelle eller organisatoriske løsningene som etter en enkeltvis og samlet vurdering av skadepotensialet og nåværende og fremtidig bruk gir de beste resultater, så sant kostnadene ikke står i et vesentlig misforhold til den risikoreduksjonen som oppnås.

[226] Strålevernforskriften § 9.
[227] Smittevernforskriften, 17. juni 2005 nr. 610 § 2-1(1) siste punktum.
[228] Støyforskriften, 26. april 2006 nr. 456, er hjemlet i arbeidsmiljøloven [2005] § 3-1 (hovedbestemmelsen om HMS-arbeid).
[229] EP/Rdir 2003/10/EF. Tiltakene i forskriftens § 10 ligger nær opp til direktivets artikkel 5.

> Dersom man mangler tilstrekkelig kunnskap om hvilke virkninger bruk av de tekniske, operasjonelle eller organisatoriske løsningene kan ha for helse, miljø eller sikkerhet, skal det velges løsninger som reduserer denne usikkerheten.[230]

Det er imidlertid ikke spesielt vanlig at kravene til de risikoreduserende tiltakene uttrykkes i så konkrete former. Et problem med å gi for klare føringer om tiltakenes art og styrke, er at det kan gå på bekostning av den logiske forbindelsen mellom vurdert risiko og avhjelping.

4.3.4.1 Disiplinering av ansatte

Når det er arbeidstakerne som er identifisert som en risikofaktor, blir systematiske risikoreduserende tiltak spesielt problematisk. Opplæring for å redusere faren for menneskelige feil er en type tiltak som det er greit å plassere innenfor idealtypen, det inngår i virksomhetens systemansvar. Det finnes imidlertid også situasjoner der illojalitet, langs hele skalaen mellom svak respekt for overordnedes pålegg til kriminelle anslag mot virksomheten eller mot virksomhetens evne til å etterleve plikten til å ivareta et samfunnshensyn, er en del av den risikoen man ser behov for å redusere. Når arbeidstakers lojalitet er risikofaktoren, er det glidende overganger mellom hva som hører inn under metodetrinnet organisering, og hva som hører inn under risikoreduksjon.[231]

Det ligger noen dilemmaer i å skulle håndtere illojalitet som risikoreduserende tiltak innenfor et internkontrollsystem. Forholdet er da et annet enn om en arbeidstaker begår straffbare handlinger som vedkommende selv må svare for. Spørsmålet blir hvorvidt virksomheten skal, eller kan, disiplinere sine ansatte innenfor det systematiske rammeverket. En grenseoppgang, som kan være vanskelig i praksis, er hvorvidt det er den ansatte som er illojal mot virksomheten, eller virksomheten som er illojal mot samfunnshensynet.[232] Et mer pragmatisk spørsmål er om ansattes medvirkningsplikt ved utformingen av internkontrollsystemer vil bidra til å legge en demper på eventuelle ønsker virksomheten måtte ha om å etablere overvåkning og kontroll av arbeidstakere som et risikoreduserende tiltak.

Et tredje dilemma, som i seg selv har mange sider, er hvorvidt sanksjoner mot «mildere grader» av illojalitet er egnet til å inngå i et internkontrollsystem. Ved alvorlige grader av

---

[230] Rammeforskrift for petroleumsvirksomheten, 31. august 2001 nr. 1016 § 9(2) og (3).

[231] Internkontroll for å sikre forsvarlig legemiddelhåndtering er et eksempel der både organisatoriske bestemmelser, «[virksomhetsleder skal sørge for internkontroll, herunder:] Gi skriftlige bestemmelser om hvem som kan håndtere legemidler og gjøre disse bestemmelser kjent i virksomheten» forskrift om legemiddelhåndtering, 3. april 2008 nr. 320 § 4(5)(a), og konkrete tiltak som «oversikter over innkjøpte legemidler», § 4(5)(d), må inngå blant de risikoreduserende tiltakene.

[232] Dette er et sentralt tema i vurderinger av om en virksomhet ilegges skal foretaksstraff, straffeloven [1902] § 48a.

illojalitet kan i verste fall oppsigelse være en mulig konsekvens. Det ville imidlertid fremstå som nærmest absurd å legge opp til oppsigelse av arbeidstaker som et alminneliggjort, systematisk risikoreduserende tiltak i et internkontrollsystem. Ved mildere grader av illojalitet er det antakelig mulig å etablere rutiner for advarsler eller lignende milde reaksjoner, men det kan likevel være tvilsomt om det er hensiktsmessig og gjennomførbart. Spørsmål om illojalitet har stått mest på spissen i situasjoner med motstrid mellom lojalitetsplikten og arbeidstakers ytringsfrihet. Det er da svært sterke hensyn som taler for at lojalitetsplikten må ha sine grenser.[233] Terskelen er imidlertid ikke nødvendigvis høy for mindre alvorlige sanksjoner ved mindre alvorlige pliktbrudd.[234] En positiv effekt, som sanksjoner mot ansatte som del av internkontrolltiltakene kanskje kunne ha, er at det ville fremme formelle og etterrettelige sanksjoner. Uformelle og fordekte sanksjoner, som å frata en ansatt oppgaver eller å hindre forfremmelser, ville være både etisk og praktisk umulig å innføre som systematiske og planlagte tiltak.

Innen informasjonssikkerhet finnes det, i moderat form, forventninger om at disiplinering av arbeidstakere skal inngå i de systematiske, risikoreduserende tiltakene. En bakgrunn for dette kan ligge i at styringssystemer for informasjonssikkerhet har et sammensatt internasjonalt opphav. Metodikken, som ligger nært opptil idealtypen risikobasert internkontroll, er blant annet utbredt i multinasjonale selskaper og faget utvikles i stor grad i internasjonale fora. I den toneangivende standarden for styring av informasjonssikkerhet, som anbefaler ulike ledd i et prosedyreverk i et samspill med tekniske sikkerhetstiltak, er anbefalingen for disiplinære reaksjoner utformet slik:

> Det bør foreligge en formell disiplinærprosess for ansatte som har forbrutt seg mot organisasjonens sikkerhetsforskrifter og prosedyrer. En slik prosess kan avskrekke ansatte som ellers ville blitt fristet til å omgå sikkerhetsprosedyrer. I tillegg bør den

[233] Dette er tydelig understreket ved at den ansattes vern mot gjengjeldelse ved varsling skal legges til rette for i det systematiske helse-, miljø- og sikkerhetsarbeidet, arbeidsmiljøloven [2005] § 3-6 jf. § 2-5.

[234] Jf. Kyrre Eggen (2004): «Ansattes ytringsfrihet. Rettslige bånd eller gyldne lenker?». I: *Arbeidsrett,* s. 2–23: «Det gjelder et proporsjonalitetsprinsipp i forholdet mellom graden av den ansattes pliktbrudd og konsekvensene av slike brudd. For sanksjoner i form av advarsel og lignende kreves det neppe noe mer enn et brudd på lojalitetsplikten.» Det er imidlertid vanskelig å iverksette stort strengere sanksjoner enn advarsler, det er nemlig trukket en grense for arbeidsreglementer: «I arbeidsreglementet kan ikke fastsettes bøter for forseelser mot reglementet.» arbeidsmiljøloven [2005] § 14-16(2) første punktum. Man må anta at denne begrensningen også ville gjelde dersom virksomheten skulle innarbeide sanksjoner mot brudd på arbeidsgivers selvvalgte risikoreduserende tiltak i internkontrollsystemet. Det er derfor vanskelig å se hvordan internkontrollsystemet skal kunne egne seg særlig godt for å disiplinere ansatte gjennom negative sanksjoner.

> sikre, korrekt, rettferdig behandling av ansatte som er mistenkt for alvorlige eller vedvarende sikkerhetsbrudd.[235]

Personopplysningsforskriftens sikkerhetskapittel, som er faglig forankret i en tidligere versjon av ovennevnte standard, inneholder ingen direkte pålegg om at styringssystemet skal omfatte disiplinærprosess mot ansatte som bryter interne retningslinjer. Eksistensen av en slik prosess er imidlertid antydet indirekte i Datatilsynets veiledende kommentar til sikkerhetsbestemmelsene.[236]

For helsesektoren er det utarbeidet en bransjenorm for informasjonssikkerhet, som skal sikre et felles sikkerhetsnivå horisontalt mellom virksomheter som samhandler elektronisk i Norsk helsenett. Å etterleve bransjenormen er oppstilt som et vilkår for virksomheter som deltar i helsenettet. Denne bransjenormen går noe lenger i å stille krav til disiplinærprosess: «Brudd på *taushetsplikten* skal som konsekvens minimum medføre en *advarsel* for den som begår bruddet, og bruddet skal behandles iht. avviksprosedyre.»[237]

Krav til formelle disiplinærprosesser mot ansatte som bryter interne prosedyrer er imidlertid ikke noe vanlig innslag i internkontrollpliktene i norsk lovgivning.

4.3.5 Egen kontroll med at tiltakene fungerer

Virksomhetens egen overvåkning og etterprøving av internkontrollprosessen er ofte nevnt på et eller annet vis i forskriftsbestemmelser, uten nærmere føringer for kontrollenes innhold og omfang. I den generelle internkontrollforskriften, er det oppstilt en tabell over internkontrollens innholdselementer og dokumentasjonskrav.[238] Andre begreper, som internrevisjon, sikkerhetsrevisjon eller tilsvarende, brukes også om dette metodetrinnet.[239]

---

[235] NS-ISO/IEC 17799:2005. Denne standarden er videreført, uten innholdsmessige endringer, med nummeret NS-ISO/IEC 27002. Standarden anbefaler også at reaksjonsformer ved brudd på krav til sikkerhet tas inn i virksomhetens ansettelsesvilkår.

[236] Kommentaren til personopplysningsforskriftens § 2-9, virksomhetens plikt til å pålegge medarbeidere taushetsplikt om forhold som har betydning for informasjonssikkerheten, understreker at virksomheten «pålegges å informere medarbeideren … om de konsekvenser – både *for egen del*, for den behandlingsansvarlige, og for de personer opplysningene kan knyttes til – brudd på taushetsplikten kan medføre.» *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer*. (2000), s. 11 (min utheving).

[237] Sikkerhetsnormen, s. 19. Uhevede ord i bransjenormen er definert i dens innledningskapittel, *advarsel* er definert som «en skriftlig reaksjon fra virksomheten overfor en ansatt som har brutt prosedyrer e.l.» Bransjenormen er en videre detaljering av systematikken og kravene i personopplysningsforskriftens sikkerhetskapittel, og kan betraktes som et «halvfabrikat» internkontrollsystem. Virksomheten skal utarbeide sitt internkontrollsystem som ellers etter kravene i helseregisterloven § 16 og personopplysningsforskriftens kapittel 2, med de moderate føringene for mål, akseptabel risiko og risikoreduserende tiltak som ligger i bransjenormen.

[238] Det siste elementet i tabellen er å «foreta systematisk overvåkning og gjennomgang av internkontrollen for å sikre at den fungerer som forutsatt; må dokumenteres skriftlig.» internkontrollforskriften [1996] § 5(8).

[239] Jf. for eksempel forskrift om risikostyring og internkontroll for finansvirksomheter eller sikkerhetsnormen for sikring av helseopplysninger i helsetjenesten.

En systematisk gjennomgang av internkontrollsystemet handler ikke primært om å avdekke enkeltstående feil eller avvik, det dekkes av neste metodetrinn. Hensikten er systemforbedring og organisatorisk læring. Systemforbedring er en del av internkontrollmetodikken som har sitt opphav i kvalitetskontrollmetoder. Dette kan således ses som et innlån fra en litt annen variant av internkontrollmetodikken enn en rendyrket risikobasert internkontroll. Tilsynsorganenes veiledninger og opplæringsmateriell setter i mange tilfeller likhetstegn mellom kvalitetssikring og internkontroll. I enkelte veiledningsdokumenter, som i utgangspunktet forklarer et bestemt internkontrollregelverk, er beskrivelser av kvalitetssikringsmetoder og sykliske forbedringsprosesser viet like stor plass og oppmerksomhet som de rettslige pliktene. Dette kommer særlig til syne innen helse- og sosialområdet, der veiledninger til flere internkontrollforskrifter presenterer og forklarer «the Deming Wheel», et opplegg for syklisk kvalitetsforbedring med opphav i internasjonal kvalitetssikringslitteratur.[240] Selve det sykliske elementet i idealtypisk internkontroll har ofte svakt belegg i lov og forskrift, men forsterkes gjennom metodelitteraturen og veiledninger. Det er primært i de faglig-administrative veiledningsdokumentene at koblingen mellom internkontrollsystemer og kvalitetssikringssystemer synliggjøres.[241] Forventningen er at resultatene fra virksomhetens egne revisjoner eller gjennomganger av internkontrollsystemet skal tas med i stadig nye versjoner, eller runder, av metodetrinnene i internkontrollprosessen.

Selv om kontroll og systematiske gjennomganger gjerne er uttrykte plikter, er systemforbedring som sådan oftest et implisitt forventet resultat. Det finnes imidlertid eksempler på at systemforbedring er uttrykt som en eksplisitt plikt.[242] En eksplisitt plikt til systemfor-

[240] Et eksempel er veiledningen til forskrift om kvalitet i pleie- og omsorgstjenestene, 27. juni 2003 nr. 792. Forskriften i seg selv stiller krav til prosedyrer for å sikre at man ivaretar angitte kvalitetsmål som pasienten skal kunne forvente. Veiledningen utlegger dette som et syklisk kvalitetsforbedringsarbeid, *Kvalitet i pleie- og omsorgstjenestene.* (2004), s. 33: «Rigide prosedyrer kan virke hemmende på den individuelle tilpasningen av tjenestene. Arbeidet med kvalitet skal være en kontinuerlig prosess. Her kan prosessen i Demings kvalitetssirkel være en nyttig måte å arbeide kontinuerlig med å forbedre kvaliteten i pleie- og omsorgstjenestene. Demings sirkel viser en kontinuerlig prosess, der vi først planlegger et forbedringstiltak, gjennomfører planen, for så å kontrollere resultatene og deretter korrigerer praksis på ny.»

[241] Se for eksempel *Hvordan holde orden i eget hus: Internkontroll i sosial- og helsetjenesten*, s. 28: «Internkontrollens formål er å sikre etterlevelse av sosial- og helselovgivningen gjennom systematisk styring og kontinuerlig forbedring. Det finnes mange ulike modeller som illustrerer systematisk forbedringsarbeid. En av disse er 'Demings sirkel' (Dr W. E. Deming).» Et annet eksempel er *Internkontroll i barneverntjenesten i kommunene – en veileder*, s. 10: «Når internkontroll er etablert må det foretas rutinemessige gjennomganger av om de fastsatte prosedyrer eller andre tiltak er i samsvar med regelverket og etterleves i praksis. Dette kan for eksempel gjøres ved at bestemte prosedyrer gjennomgås i plenum/allmøte en eller flere ganger i året. Slike felles gjennomganger kan ofte føre til at det avdekkes behov for justeringer/forbedringer.» Hele denne prosessen oppsummeres, på s. 19, ved å vise til «Demings sirkel».

[242] Jf. kravet om at petroleumsvirksomheten «skal foregå slik at et høyt sikkerhetsnivå kan opprettholdes og utvikles i takt med den teknologiske utvikling», petroleumsloven [1996] § 9-1.

bedring kan forstås på to måter. Den ene er som understreking av internkontrollsystemets sykliske karakter, den andre er som en understrekning av fleksibilitet, at målet er bevegelig.

4.3.6 Avvikshåndtering

Det siste metodetrinnet i risikobasert internkontroll som reguleringsmetode er å håndtere feil og avvik. Mens både risikoreduserende tiltak og sykliske forbedringsprosesser dreier seg om å foregripe og forebygge avvikene, er avvikshåndtering et uttrykk for en resiliensstrategi. En viss toleranse for avvik skjerper evnen til å forstå og tilpasse seg endringer i risikobildet. God avvikshåndtering er i seg selv en prosess for organisatorisk læring, men av en annen karakter enn systematiske gjennomganger av systemet.

I et idealtypisk internkontrollsystem er avvik påregnelige. Virksomheten har selv besluttet kriteriene for akseptabel risiko. Det er imidlertid selvfølgelig ikke slik at en virksomhet bare vil oppleve hendelser som ligger innenfor akseptert risiko. Menneskelige feil, ytre hendelser, tilsiktede brudd på retningslinjer med mer vil også av og til ha konsekvenser som er mer alvorlige enn det virksomheten har valgt å akseptere.

Avvik er i seg selv et vagt begrep. Virksomheten må konkretisere og presisere innholdet gjennom arbeidet med å utforme internkontrollsystemet. Flere faktorer, som virksomhetens art, hvilke risikofaktorer som er identifisert og hvordan de vektlegges, faglige tradisjoner og organisasjonskultur etc., kan påvirke den enkelte virksomhets oppfatning av hva et avvik er, og av hvor alvorlig det er. I mange sammenhenger vil det som menes med avvik være konkrete brudd på de interne rutinene, eller de risikoreduserende tiltakene.[243] På noen områder er det egne pålegg i lov om å melde fra om alvorlige enkelthendelser. Arbeidsulykker der en arbeidstaker omkommer eller blir alvorlig skadet skal meldes til Arbeidstilsynet.[244] Et annet slikt pålegg er at Helsetilsynet i fylket skal ha melding både om betydelig personskade på pasient og om «hendelser som kunne ha ført til betydelig personskade».[245]

[243] En slik oppfatning ligger til grunn i personopplysningsforskriften: «Bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik», og at Datatilsynet skal varsles «dersom avviket har medført uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig.» personopplysningsforskriften § 2-6(1) og (3). Tilsvarende plikt til å melde særskilt uheldige eller konsekvensrike avvik til vedkommende statlige tilsynsorgan finnes også på andre områder.
[244] Arbeidsmiljøloven [2005] § 5-2.
[245] Spesialisthelsetjenesteloven § 3-3. Selv om lovteksten ikke knytter denne meldeplikten til internkontrollsystemet, er en slik kobling gjort i forarbeidene: «Den viktigste endringen som nå foreslås er en utvidelse av meldeplikten til også å omfatte hendelser som kunne ha medført betydelig skade. En slik utvidelse av meldeplikten må ses på som en viktig del av institusjonens internkontroll.» Ot.prp. nr. 10 (1998-1999), kapittel 6.3.3.

Det er liten uenighet om at avvikshåndtering er viktig. Empiriske studier viser imidlertid at underrapportering av avvik er en svært vanlig situasjon.[246] Svakheten i dette metodetrinnet er altså neppe at det er vanskelig å forstå eller å se nytteverdien, men at det er praktisk vanskelig å fange opp avvikene og få dem underlagt de rutinene virksomhetene måtte ha for å håndtere dem. I internasjonal litteratur om internkontroll og andre former for selvregulering er et åpenbart dilemma ved avviksrapporteringsrutiner, «the blame game», hyppig diskutert. Den som er nærmest til å rapportere avviket internt i virksomheten, er ofte også den som risikerer mest dersom avviket blir kjent. Selv om en oppegående virksomhetsledelse forstår at avvik må fanges opp før de kan håndteres, er det vanskelig å gi arbeidstakere tilstrekkelig trygghet for at rapporteringen ikke får negative følger. En del virksomheter har forsøkt å løse dette ved å etablere anonyme meldekanaler. Det burde redusere problemet fra en begrunnet frykt for represalier til et spørsmål om opplæring i melderutinene og trygghet for at anonymiteten er reell.[247]

Innen helsevesenet er det et forhold som kan bidra til at frykten for å melde fra om avvik kan være noe større enn i andre sektorer. Der har tilsynsmyndigheten flere individrettede reaksjonsformer mot det enkelte helsepersonell.[248] I de mest alvorlige tilfellene kan autorisasjon, lisens eller spesialistgodkjenning tilbakekalles. Dilemmaene mellom virksomhetens plikt til å melde, og reaksjonshjemler overfor helsepersonell som arbeider i virksomhetene, er også drøftet i Helsetilsynets egne styrende dokumenter.[249]

4.4 Eksterne tilsyn

Statlige tilsynsorganer er etablert for en lang rekke ulike samfunnshensyn. Mange tilsynsorganer har et horisontalt nedslagsfelt, de skal føre tilsyn for å ivareta samfunnshensynet uavhengig av hvilken bransje eller sektor det enkelte tilsynsobjekt ellers hører hjemme i. Det gjelder for eksempel Datatilsynet, Arbeidstilsynet, Statens forurensningstilsyn og mange flere.

---

[246] Jf. Nina Husom (2002): «Helsevesenet trenger en medisinsk havarikommisjon». I: *Tidsskrift for Den norske legeforening,* s. 1238 og Sissel Steihaug m. fl. (2008): «Kartlegging og risikovurdering av HMS i hjemmetjenesten i bydelene Oslo kommune».

[247] I forarbeid til endringslov som innførte plikt for arbeidsgivere til å legge til rette for systematisk varsling, arbeidsmiljøloven [2005] § 3-6, ble det vurdert om det burde innføres regler som gir arbeidstakere rett til anonymitet overfor arbeidsgiver hvis de varsler om kritikkverdige forhold. Å lovfeste en slik rett ble ikke ansett hensiktsmessig, jf. Ot.prp. nr. 84 (2005-2006), s. 30. På s. 54, i kommentarene til § 3-6, anbefales imidlertid virksomhetene å vurdere om det er behov for å etablere en ordning med anonym varsling i de interne rutinene.

[248] Helsepersonelloven §§ 56–59.

[249] *Tilsyn med helsepersonell og helsevesen basert på informasjon om enkelthendelser mv. – Rettslige rammer.* (2004), s. 35.

På enkelte andre områder er det nær forbindelse mellom samfunnshensyn og tilsynsobjekters sektortilhørighet, slik tilfellet er med kredittinstitusjoner, helseinstitusjoner og næringsmiddelbransjen. Her hører tilsynsorganene til samme sektor og fagtradisjon som tilsynsobjektene.

Tilsynsorganene er forvaltningsorganer, og som sådan en del av den utøvende statsmakt. Myndighetsutøvelsen kan i visse henseender av og til karakteriseres som «domstollignende», fordi de har hjemler både til relativt inngripende undersøkelser i virksomhetene og til å iverksette sanksjoner.[250] Likevel er en forståelse av tilsynsorganenes virksomhet som domstollignende antakelig mer villedende enn den er treffende. Som del av den utøvende statsmakt er tilsynsorganene mer politiserte. En sosiologisk artikkel som analyser Kredittilsynets kontrollvirksomhet, og omlegging til internkontrollbaserte tilsynsmetoder, tolker denne omleggingen som elementer i en mer aktiv og regulerende stat, til tross for at metodikken gir tilsynsobjektene større handlingsrom.[251]

4.4.1 Tilsynsmetoder

I de senere år har det funnet sted en stor omlegging og ensretting av statlige tilsynsorganers tilsynsmetoder. Til dels kan dette kanskje ses som dannelsen av en «tilsynsprofesjon».[252] De som arbeider med tilsyn begynner å betrakte det som et fag i seg selv, med spesialiserte metoder og en egen rolleforståelse. Kunnskaper om og erfaringer med å gjennomføre tilsyn overfor virksomheter blir etter en slik profesjonslogikk vel så viktig for å ivareta samfunnshensynet som den konkrete fagkunnskapen om brannhemmende materialer, kryptering av datatrafikk eller støyskader i arbeidslivet.[253]

Den viktigste nyskapningen i statlige tilsynsorganers etterprøving av en virksomhets internkontroll er en systemrevisjon. Dette innebærer at tilsynsorganet kontrollerer at internkontrollsystemet er etablert i tråd med regelverket, og at det etterleves og vedlikeholdes. Aaslandutvalget, som leverte en utredning om statlig tilsyn med kommunesektoren, særlig

[250] Internkontrollsystemet er en del av virksomhetens «bevisførsel» overfor tilsynsorganet. «Et slikt internkontrollkrav kan ses som en plikt til å bevise at virksomheten etterlever de krav som er satt.» Hans Petter Graver (2004): «Bevisbyrde og beviskrav i forvaltningsretten». I: *Tidsskrift for Rettsvitenskap,* s. 465–498.

[251] I artikkelens konklusjon hevedes det at «begrepet om *deregulering*, som innebærer at det blir *mindre* statlig regulering, ikke er adekvat for å beskrive den utviklingen som har skjedd.» Trond Løyning (2005): «Kredittilsynet i en neoliberal økonomi : finansmarkedenes dannelse». I: *Sosiologisk tidsskrift,* s. 335–362. (s. 357, original utheving).

[252] Det dreier seg selvfølgelig ikke om en ren profesjon i tradisjonell forstand, jf. drøftingen om individuelt helsepersonell og profesjonsautonomi, kapittel 3.2.

[253] Med en litt tvilsom referanse til uvitenskapelig «anekdotisk belegg», fra egne bekjentskaper, ser det ut til at det ikke er uvanlig at karriereløpet til personer som arbeider i et statlig tilsynsorgan er å gå videre til et annet tilsynsorgan som forvalter andre regelverk, samfunnshensyn og fagkunnskaper.

med bakgrunn i fylkesmannens oppgaveportefølje, gir følgende kortfattete beskrivelse av metoden:

> Systemrevisjon retter kontrollen mot at virksomheten kan dokumentere at de har bygd opp et internkontrollsystem, og at dette fungerer i praksis. Ideen er å finne fram til svakheter i systemet istedenfor å fokusere på enkeltstående feilgrep.[254]

Den gjenstanden som primært undersøkes er dokumentasjon. En systemrevisjon går imidlertid ofte lenger enn bare å være en ren dokumentverifikasjon, for eksempel kan etterprøvingen også omfatte intervjuer med medarbeidere eller stikkprøver av de tiltakene som er beskrevet i virksomhetens dokumentasjon.

Selv om systemrevisjon er hovedprinsippet for ekstern etterprøving av internkontroll, vil tilsynsorganene sjelden være avskåret fra å utøve andre typer kontrollaktiviteter. En betegnelse som ofte brukes om motstykket til systemrevisjon er hendelsesbasert tilsyn. Forskjellen ligger i at det da er ett eller flere konkrete forhold som har initiert tilsynet, og kartlegging av hendelsene er en viktig del av det. I en viss forstand kan dette betraktes som at tilsynsorganet involverer seg i virksomhetens avvikshåndtering i en konkret sak. Det er likevel flere likheter enn forskjeller mellom disse tilsynsmetodene. Et hendelsesbasert tilsyn vil i mange tilfeller også omfatte kontroll med virksomhetens internkontrollsystem, for å vurdere om hendelsen har sammenhenger med systemmessige svakheter. Hendelsen er da en utløsende årsak, mens den videre gangen i tilsynet følger samme metoder som systemrevisjon. Både tilsynsorganets hjemler for å innhente opplysninger og sanksjonsmulighetene vil være de samme uavhengig av tilsynsmetode.[255]

Ulike typer hendelser kan utløse tilsyn. Bakgrunnen for et hendelsesbasert tilsyn er at tilsynsorganet får kunnskap om noe som er kritikkverdig. En mulig kilde er de hendelsene tilsynsobjektet selv rapporterer inn, som følge av lovpålagt meldeplikt eller som ledd i virksomhetens rutiner for avvikshåndtering. En annen kilde kan være klager som tilsynsorganet mottar fra skadelidte eller fra interessentgrupper, etter hva som er mest nærliggende ut fra det aktuelle samfunnshensynet. Et hendelsesbasert tilsyn vil ikke nødvendigvis forutsette at det foreligger en formell klagerett, klagen kan tolkes som en appell til tilsynsorganet om å undersøke saken på eget initiativ. Oppmerksomhet om en sak i medier og opinion kan

[254] NOU 2004:17, s. 53.

[255] En kvalitativ undersøkelse, der blant annet nøkkelpersonell i en del kommuner ble spurt om deres erfaringer med det statlige tilsynet med kommunens virksomhet, viste at hendelsesbaserte tilsyn generelt ble oppfattet som mer negativt enn systemrevisjoner, Gro Sandkjær Hanssen m. fl. (2004): «Statlig tilsyn med kommunesektoren». Disse erfaringene hang nettopp sammen med måten tilsynet ble initiert på, som en reaksjon på negativ oppmerksomhet om konkrete forhold.

på samme vis også være en spore til et tilsynsbesøk. I noen tilfeller skal arbeidstakere eller bestemte funksjoner i en virksomhet varsle myndighetene om kritikkverdige forhold.[256] Der en slik adgang ikke er hjemlet, vil det i utgangspunktet være illojalt å varsle myndighetene, før interne kanaler for varsling innad i virksomheten er uttømt.[257]

Et av spørsmålene som Aaslandutvalget vurderte var om ikke bare hjemlene for å utøve tilsyn, men også tilsynsmetoden som sådan, burde lovreguleres. Utvalgets konklusjon på dette spørsmålet var at de ikke anbefalte lovregulering av tilsynsmetoder.[258]

4.4.2 Samordning av tilsynsvirksomheten

Mange virksomheter må forholde seg til flere forskjellige internkontrollplikter, og til ulike tilsynsorganer. For eksempel kan en virksomhet i næringsmiddelbransjen være omfattet av plikt til internkontroll både etter næringsmiddellovgivningen, arbeidsmiljølovgivningen og personopplysningslovgivningen. En virksomhets handlingsrom, som i prinsippet kan være stort innen hvert av disse områdene, kan likevel bli snevert i praksis fordi virksomheten selv må forene og avveie de ulike samfunnshensynene bak hver av internkontrollpliktene på en måte som alle de involverte tilsynsorganene vil finne akseptabel.

Behovet for å samordne tilsynene har vært på agendaen for ulike utredninger og politiske initiativer siden tidlig på 1990-tallet.[259] Påpekningen av behovet har riktignok handlet mer om arbeidsbelastning og tilsynsslitasje enn om faren for inkonsistente signaler fra forskjellige tilsynsorganer eller en utilsiktet tilstramming i den fleksibiliteten som ligger i hvert av de internkontrollbaserte regelverkene. Tilsyn som ikke samordnes blir i praksis tilsynsobjektets problem.

En del aktivitet har pågått, og pågår fremdeles, for å samordne tilsynsvirksomhet. Den prosaiske varianten av samordning er at tilsynsorganer av og til slås sammen. Det kan imidlertid, også innen ulike, nært beslektede samfunnshensyn, være ønskelig å opprettholde flere, faglig spesialiserte tilsynsorganer. Det har vært eksempler på etablering av samarbeid mellom forskjellige tilsynsorganer innen samme kategori av samfunnshensyn, uten å forankre samord-

[256] For eksempel helsepersonelloven § 17.
[257] Antakelig vil det likevel være legitimt å varsle relevant tilsynsorgan om kritikkverdige forhold dersom virksomheten ikke har innarbeidet rutiner som legger forholdene til rette for varsling, jf. arbeidsmiljøloven [2005] § 3-6.
[258] «Etter utvalgets oppfatning bør tilsynsmyndighetenes valg av tilsynsmetode vurderes løpende og i tillegg tilpasses det enkelte tilsynsområde og den enkelte situasjon. Etter utvalgets oppfatning er det av den grunn uheldig å lov- eller forskriftsfeste tilsynsmetodikk.» NOU 2004:17, s. 117.
[259] Noen av disse initiativene er beskrevet i Ot.prp. nr. 67 (1999-2000).

ningen i den formelle reguleringen.[260] En modell for å samordne tilsyn som formaliseres i regelverket, er å gi et av de aktuelle tilsynsorganene ansvar for å samordne tilsynsaktiviteten. Denne modellen er formalisert i regelverket på to områder.[261] En alternativ variant er å lovfeste en form for kjøreregler mellom tilsynsorganene innen et område. Denne modellen finnes, i en relativt moderat form, i helseforskningsloven.[262] Nylennautvalget, som foreslo loven, var opptatt av at forskerne normalt bare skulle behøve å forholde seg til én «postkasse», men så likevel et klart behov for at tilsynsorganene måtte ha full anledning til etterhåndskontroll med sine ansvarsområder.[263] Blant annet har både Helsetilsynet og Datatilsynet anledning til å gi pålegg på sine områder. Kravet til samordning er formalisert som en plikt til å orientere andre tilsynsorganer om de pålegg som gis.[264]

Samordningsproblemet tiltar når ulike kategorier av samfunnshensyn står mot hverandre. Et problem som har kommet på spissen flere ganger er arbeidsgivers overvåkning av arbeidstakeres kommunikasjon, innsats eller resultater. Mot styringsinteressen står en sammensatt verneinteresse, både for den ansatte i egenskap av arbeidstaker og som autonomt individ. Regelverket hører dels hjemme under arbeidsmiljøloven, og dels under personopplysningsloven. Både Arbeidstilsynet og Datatilsynet er tilsynsmyndighet.[265]

Når samordning på tilsynsnivå ikke er egnet til å bygge bro over så ulike verneinteresser, kan det være nærliggende å samordne interessene konkret i regelverket i stedet, noe som kan ha den kostnad at reguleringen blir mindre fleksibel. Med endringsforskrift 29. januar 2009

[260] Et eksempel er arbeidstakervern, og begrepet «HMS-etatene». Dette er omtalt i tilsynsmeldingen fra 2003: «Det er Arbeids- og administrasjonsdepartementets erfaring at samordning og koordinering på tvers av tilsynsvirksomhetene har økt, men det er fortsatt et stort potensial for forbedring innenfor det opprettede HMS-samarbeidet. Etter departementets vurdering beror manglende samordning på at det fremdeles er for store barrierer knyttet til at etatene er egne organisasjoner, som i mange tilfeller ønsker å rendyrke sine særtrekk og sitt regelverk.» Stortingsmelding nr. 17 (2002-2003), s. 43.

[261] Det ene er at Petroleumstilsynet skal koordinere tilsyn der tilsynsobjektet tilhører petroleumssektoren, etter ulike regelverk og samfunnshensyn. Instruks om Petroleumstilsynet, 19. desember 2003 nr. 1594. De andre er at Direktorat for samfunnssikkerhet og beredskap skal samordne tilsyn der verneinteressen er samfunnssikkerhet, overfor virksomheter med «storulykkepotensial». Storulykkeforskriften, 17. juni 2005 nr. 672.

[262] Helseforskningsloven, innfører som hovedprinsipp (§§ 9 og 10) at regionale komité for medisinsk og helsefaglig forskningsetikk skal forhåndsgodkjenne forskningsprosjekter, med vurderinger som også omfatter forskningsprosjektets rettslige grunnlag for å behandle helseopplysninger. Det enkelte forskningsprosjekt skal altså ikke behøve å gå i «stafett» mellom tilsynsorganer på forhånd.

[263] «En samordnet myndighetsmodell gjør ikke at alle andre forvaltningsorganer sjaltes ut. Statens helsetilsyn, Statens legemiddelverk og Datatilsynet, har på sine områder bygd opp unik kompetanse som utvalget vil bygge videre på i et mer samordnet system. Men det kan ikke være slik at alle saker 'automatisk' må bli behandlet av alle myndigheter. Forvaltningsorganene må stole på hverandres vurderinger, og de må samarbeide slik at virksomhetene effektiviseres.» NOU 2005:1, s. 137.

[264] Helseforskningsloven § 51(3): «Når Statens helsetilsyn har gitt et pålegg, skal øvrige tilsynsmyndigheter informeres om dette såfremt forskningsprosjektet også faller inn under deres tilsynsområde,» og tilsvarende i § 52(3): «Når Datatilsynet har gitt et pålegg, skal Statens helsetilsyn informeres om dette.»

[265] Personvernkommisjonen mente i sin rapport at «plasseringen av disse reglene vil skape utfordringer i praksis. Etter kommisjonens oppfatning bør regler for innsyn i og kontroll av e-post og dokumenter legges til partenes lov; nemlig arbeidsmiljøloven, alternativt i en egen personvernlov for arbeidslivet.» NOU 2009:1, s. 156.

nr. 84 fikk personopplysningsforskriften et nytt kapittel 9, om arbeidsgivers rett til innsyn i arbeidstakers e-postkasse og dokumenter lagret på personlig område i arbeidsgivers nettverk.[266] Datatilsynets tidligere praksis på området, og et forskriftsutkast fra 2006 som fikk så hard medfart i høringsrunden at det ikke ble vedtatt, hadde som utgangspunkt at slikt innsyn skulle baseres på virksomhetens egne beslutninger, etablering av rutiner og tiltak som sikrer godt samsvar mellom virksomhetens praksis og de forventninger arbeidstakerne med rimelighet kunne ha om sin arbeidsgivers praksis.[267] Det nye kapittel 9 i personopplysningsforskriften er derfor universelle vilkår for innsyn og prosedyrer ved innsyn, som er en grei detaljering av plikter og rettigheter etter personopplysningsloven, men uten den fleksibiliteten som tidligere praksis på området gjorde mulig.[268]

Et eksempel på forsøk på å få til samordning gjennom regelverket som ikke har lykkes, og der forslaget om samordning ble frafalt, er reglene om forsikringsselskapers håndtering av helseopplysninger.[269] Nesten åtte år etter utredningen kom proposisjonen som behandlet forslagene videre. Mange av de materielle forslagene om behandling av helseopplysninger ble tatt til følge, men forslaget om en plikt til kvalitetssikringssystem som forente de ulike hensynene på tvers av samfunnshensyn og tilsynsorganer, ble forkastet.[270]

Samordning på et så omfattende nivå som drøftet ovenfor, gjennom tilsynssamordning eller felles regelverk, dreier seg om hele det kompliserte spørsmålet om hva hvert tilsynsorgan anser som gode nok internkontrollprosesser hos samme tilsynsobjekt. Det omfatter likheter og

---

[266] Forskriftsendringen ble gitt i medhold av en ny bestemmelse, vedtatt for dette formålet, i arbeidsmiljøloven: «Arbeidsgivers rett til innsyn i arbeidstakers e-post mv. reguleres i forskrift gitt i medhold av personopplysningsloven § 3 fjerde ledd første punktum.» arbeidsmiljøloven [2005] § 9-5.

[267] Forslaget fra 2006 la opp til fleksibel selvregulering, som anerkjente ulike typer virksomheters ulike behov, men som forutsatte at hver virksomhet tok stilling til spørsmålet og fulgte opp med eget regelverk, dette ble understreket i høringsnotatet ved å anbefale arbeidsgiverne å utarbeide *instruks*: «Datatilsynet anbefaler at virksomheter utformer en datainstruks som bl.a. omfatter regler for innsyn i e-post. Dersom virksomheten har vedtatt en slik instruks er det viktig at denne følges ved gjennomføring av innsynet. Det vil si at arbeidsgiver forholder seg til de situasjoner som er angitt som saklig begrunnelse for innsyn, og at man følger de fremgangsmåter og metoder som instruksen beskriver. Dersom instruksen er fulgt, vil interesseavveiningen som regel falle ut til fordel for arbeidsgiver, forutsatt at instruksen ikke gir større rett til innsyn enn det personopplysningsloven gir grunnlag for.» *Forslag til regler om arbeidsgivers tilgang til Ansattes e-post mv. – endring av personopplysningsloven § 3 og § 46, nytt kapittel i personopplysningsforskriften og ny bestemmelse i arbeidsmiljøloven.* (2006), s. 6.

[268] Det eneste unntaket fra det universelle grepet er at «reglene gjelder så langt de passer for universiteters og høyskolers innsyn i studenters e-postkasse, og for organisasjoners og foreningers innsyn i frivilliges og tillitsvalgtes e-postkasse», personopplysningsforskriften § 9-1(5).

[269] Følgende ordlyd ble foreslått innført som ny bestemmelse i forsikringsavtaleloven, 16. juni 1989 nr. 69: «Departementet kan bestemme at selskapet skal etablere og dokumentere rutiner som sikrer at opplysninger om helseforhold håndteres og vurderes på en betryggende og faglig forsvarlig måte.» Selv om ordlyden ikke sier stort i seg selv, var dette et forslag om et internkontrollsystem, som forente aktuarmessig risiko, helsevurderinger, og personvernhensyn. Det var en drøfting i utredningen av hvilket organ som kunne være aktuell tilsynsmyndighet for dette kvalitetssikringssystemet, både Kredittilsynet, Helsetilsynet og Datatilsynet ble ansett som delvis relevante. NOU 2000:23, s. 86.

[270] Departementet mente at «behovet for å etablere et eget kvalitetssikringssystem foreløpig ikke synes å forsvare de administrative og økonomiske konsekvensene dette vil ha.» Ot.prp. nr. 41 (2007-2008), s. 84.

forskjeller i tolkning av regelverk, synet på hvilken aksept av risiko man anser det nødvendig å overprøve, kultur og praksis for bruk av virkemidler som innsynshjemler, pålegg og sanksjoner med mer. En enklere innfallsvinkel enn samordning er å gjennomføre felles tilsynsbesøk. To tilsynsorganer kan være interessert i å undersøke samme, eller noenlunde samme, del av en virksomhet fra hvert sitt ståsted. Et eksempel kunne være håndtering av farlig avfall, som skal være underlagt systemkontroll ut fra de to samfunnshensynene arbeidstakervern og miljøvern.

Et konkret tilfelle av likeartede problemstillinger der virksomheten er underlagt ulike sett av reguleringer som røktes av hvert sitt statlige tilsynsorgan er pasienters konfidensialitetsvern. Helsetilsynet fører tilsyn med helserettens regler om taushetsplikt, mens Datatilsynet fører tilsyn med virksomhetens informasjonssikkerhet. Disse to tilsynsorganene har gjennomført felles tilsynsbesøk i helseforetak ved enkelte anledninger. Tilsyn etter bare ett av disse tilsynsorganenes ansvarsområde gir et svakt grunnlag for å vurdere hvor god beskyttelse pasienters konfidensialitet egentlig har hos virksomheten, felles tilsyn setter en større del av virkeligheten på dagsorden som et sammenhengende tema. Felles tilsynsbesøk kan ha betenkelige sider, fordi tilsynsorganene da forutsetter at virksomheten gjennomfører det arbeidet med å skape sammenheng i regelverket som lovgiver ikke har lyktes med.

Det de litt spredte ekseplene på ulike varianter av samordning egentlig viser er, dessverre, at samordningsproblemet i hovedsak ikke har funnet gode og enhetlige løsninger. For tilsynsobjektene er faren stor, både for inkonsekvente myndighetssignaler og for arbeidskrevende oppfølging av tilsynsresultater. Manglende samordning er fremdeles et relativt omfattende problem i det statlige tilsynet med virksomhetenes internkontroll. Det kan henge sammen med at samordningsproblemet peker mot et litt dypere problem. Til tross for ambisjonene om helhet og sammenheng, virker internkontroll sementerende for vertikale styringsprosesser, virksomhetsgrenser, kompetansegrenser og relativt snevre kategorier av samfunnshensyn. Risikobasert internkontroll synes å være mer til hinder enn til hjelp for horisontalt samarbeid mellom virksomheter og for samordning av arbeidet med forskjellige samfunnshensyn innen en virksomhet.

4.4.3 Uavhengig kontroll og rollen som rådgiver for virksomhetene

De statlige tilsynsorganene har i mange tilfeller en kombinert rolle som kontrollerende og rådgivende organ. Forholdet mellom tilsyn og rådgivning kan i visse sammenhenger være problematisk på grunn av den indre sammenhengen mellom metodetrinnene i et internkon-

trollsystem. Rådgivning om internkontroll er å gi råd om hvordan virksomhetens selv skal treffe beslutninger, gjennomføre risikovurderinger, og iverksette avpassede og relevante tiltak. Dersom man går langt i å gi råd om hva som for eksempel er gangbare risikoreduserende tiltak, medfører det en fare for å punktere den helhetlige systematikken. Hvorvidt et bestemt risikoreduserende tiltak er tilstrekkelig – for eksempel passordbeskyttelse eller en teknisk brannmur, dersom samfunnshensynet er informasjonssikkerhet – er det knapt mulig å ta stilling til uten å se tiltaket i en større sammenheng. Tiltakets egnethet henger sammen med de helhetlige vurderinger virksomheten gjør innenfor sitt internkontrollsystem. Det å bli for konkret i rådgivningsfunksjonen kan føre til at tilsynsorganet oppfattes slik at de gir tilsagn til et sikkerhetstiltak som de i et senere tilsynsbesøk må avvise, fordi tiltaket kanskje ikke er egnet for å avhjelpe det komplekse risikobildet som er identifisert.[271]

Uavhengighetsproblemet for statlige tilsyn er at det går en grense for når rådgivningen blir til en forhåndsgodkjenning av virksomhetens selvregulering. Følgen ville være at tilsynsorganet svekker sin egen fremtidige mulighet til å overprøve tilsynsobjektet.

4.4.4 Sammensatte styrings- og tilsynsfunksjoner

Den tilsynsrelasjonen som har vært beskrevet så langt er tilsyn i ett ledd, der et eksternt, statlig tilsynsorgan har hjemmel til å føre tilsyn direkte med tilsynsobjektet. Tilsynsorganet anses som uavhengig, selv om graden av uavhengighet for et organ under Kongens instruksjonsmyndighet alltids er diskutabel. Etter idealtypen bør det ikke være noen kobling mellom tilsynsrelasjonen og eier- eller styringsrelasjonen.

Innen store deler av den kommunale forvaltning er sammenhengen mellom tilsynsrelasjon og styringsrelasjon mer kompleks. Deler av det regelverket som ulike typer kommunal virksomhet er underlagt er slik at en underordnet fagenhet skal utøve internkontroll, mens kommunen er pålagt å føre det direkte tilsynet med denne fagenhetens internkontrollsystem. Det statlige tilsynsorganet fører et indirekte tilsyn, ved å etterprøve kommunens tilsyn med sine egne underliggende virksomheter. Det statlige tilsynsorganet er da som ellers uavhengig av eier- og styringsrelasjoner. Kommunens direkte tilsyn med underliggende virksomhet er derimot ikke uavhengig på samme vis. Koblingen mellom tilsynsrelasjonen og eier- eller styringsrelasjonen er til stede og må tas med i betraktningen.

[271] Rådgivningsdilemmaet for tilsynsorganer som kontrollerer internkontrollsystemer er glimrende spissformulert i en artikkel som analyserer Kredittilsynets omlegging til denne tilsynsmetodikken: «Kredittilsynet har, av forståelige grunner, inntatt den holdningen at det ikke skal drive aktiv og forpliktende rådgivning ved å gi «fasitsvar» på løsninger … om Kredittilsynet skulle stå ansvarlig for opplegget ville Kredittilsynet ende opp med å holde tilsyn med seg selv.» Løyning (2005), s. 349.

Forbindelsen mellom styringsrelasjon og tilsynsrelasjon i kommunens tilsyn med en underliggende virksomhets internkontroll har vært et sidetema i en sak for Høyesterett, i *barnehagedommen*.[272] En privat familiebarnehage, underlagt kommunalt tilsyn og plikt til internkontroll, hadde ikke tilstrekkelig inngjerding av uteplassen, noe kommunens helsesøster hadde anmerket i en tidligere befaringsrapport. Et barn falt i en bekk utenfor området, og ble alvorlig skadet. Barnehagens assurandør hadde erkjent ansvar for skaden, spørsmålet i saken var om assurandøren kunne kreve regress hos kommunen for uaktsomhet i forbindelse med godkjennelsen av, eller tilsynet med, barnehagen. Høyesterett kom under dissens 4-1 til at det ikke var grunn til å kritisere kommunen for måten den har gjennomført tilsynet med barnehagen på, og fant at det ikke var grunnlag for å gjøre erstatningsansvar gjeldende mot kommunen.

Det som er mest interessant ved dommen i denne forbindelse er drøftingen av kommunens anførsler, om at et slikt ansvar ville undergrave «systemet med internkontroll».[273] Denne anførselen innebærer det syn at internkontroll legger metodiske føringer for hvordan tilsyn bør utøves. Førstvoterende går ikke spesielt dypt inn i denne anførselen, men bemerker at partene «har gitt uttrykk for noe forskjellig syn på omfanget av kommunens tilsynsplikt.» I den videre fremstillingen av hvordan kommunen har gjennomført tilsynet legger førstvoterende vekt på at kommunen besøkte barnehagen ved tre forskjellige anledninger. Bare ett av besøkene var formelt sett en befaring i egenskap av å være tilsynsmyndighet, også de to besøkene som ikke var tilsyn kunne imidlertid ha foranlediget initiativer fra kommunen.[274] Førstvoterende avviser dermed en funksjonsdeling som innebærer at kommunen må være uavhengig i rollen som tilsynsmyndighet. Andrevoterende, mindretallet som mente kommunen var delansvarlig, deler det synet og går mer direkte løs på kommunens anførsel om at internkontroll må innebære at kommunens styringsrelasjon og tilsynsfunksjon er uavhengig av hverandre.[275]

Internkontroll med en toleddet tilsynsrelasjon, der kommunen fører direkte tilsyn med en underliggende enhet, mens et statlig tilsynsorgan fører indirekte tilsyn med kommunen,

---

[272] Rt. 2002 s. 654.

[273] «Etter ankemotpartens syn må det trekkes vide rammer for kommunens skjønn over hva som er forsvarlig. … Dersom kommunen blir pålagt et for omfattende tilsynsansvar, vil det fullstendig undergrave systemet med internkontroll i slike virksomheter.» Rt. 2002 s. 654, på s. 659.

[274] «Selv om de to siste besøkene ikke hadde noe kontrollformål, må også de etter min oppfatning inngå i oppfyllelsen av kommunens plikt til å føre tilsyn med barnehagene. Dersom det ved disse besøkene var blitt funnet noe spesielt, ville det kunne ha dannet grunnlag for reaksjon og oppfølgning fra kommunens side.» Rt. 2002 s. 654, på s. 664.

[275] «Kommunen har anført at et ansvar for kommunen i denne saken ville komme på kant med systemet med internkontroll, som gjelder i dette og en rekke andre forhold. Kommunen måtte – hevdes det – kunne stole på at barnehagen og dens ansatte førte kontroll etter forutsetningene, og et ansvar for kommunen ville gi gale signaler og vil kunne lede til overforsiktighet. Disse synspunktene er jeg ikke enig i.» Rt. 2002 s. 654, på s. 667.

oppsto gjennom adgangen til å gi forskrifter om internkontroll etter kommunehelsetjenesteloven.[276] Etter dette er systemet slik at kommunen både styrer og fører det direkte tilsynet med sine helsevirksomheter, mens Statens helsetilsyn fører tilsyn med kommunen. Den toleddete tilsynsrelasjonen var oppe til mer prinsipiell drøfting i forarbeidene til gjeldende barnehagelov. Loven er innrettet slik at Fylkesmannen fører tilsyn med barnehageeieren, mens barnehageeieren fører tilsyn med den enkelte barnehage.[277]

En mer spesiell variant av internkontroll med en ikke-uavhengig tilsynsrelasjon finner man i delrapport 2 fra granskningen av Utlendingsdirektoratet. Granskingskommisjonen anbefaler at *faglig* styring skal baseres på internkontroll.[278] Selv om det etter denne anbefalingen ikke er lovgivningen som pålegger internkontroll, men et overordnet forvaltningsorgan, er det like fullt et tiltak myntet på å skape tillit i samfunnet. Med den klassifiseringen av samfunnshensyn som er brukt her, er det mest nærliggende å si at den faglige styringen hører til i kategorien forsvarlighet, rettssikkerhet og individers rettighetsvern.

Utgangspunktet er det alminnelige forvaltningsrettslige prinsipp om overordnede organers kontroll- og instruksjonsmyndighet. Det spesielle består i at den anbefalte oppskriften for å ivareta dette ansvaret ligger tett opp til det idealtypiske internkontrollsystem. Direktoratet skal definere og dokumentere faglige mål og virkemidler, departementet skal føre tilsyn, basert på samme metoder og rolleoppfatning som uavhengige, eksterne tilsynsorganer. Til forskjell fra den delingen av tilsynsrelasjoner man har innen deler av den kommunale forvaltningen, er granskingskommisjonens anbefaling basert på at departementets sammensatte styrings- og tilsynsfunksjon skal være den eneste tilsynsrelasjonen.[279] Internkontroll der tilsynskomponenten er basert på en form for pseudouavhengighet kan imidlertid tenkes å ha uheldige

[276] Systemet etter kommunehelsetjenesteloven er faglig tilsyn med kommunen som sådan: «Statens helsetilsyn fører medisinsk-faglig tilsyn med at kommunene fremmer helsetjenestens formål på forsvarlig og hensiktsmessig måte.» kommunehelsetjenesteloven § 6-3. Dette innebar imidlertid ikke i utgangspunktet at plikten til internkontroll (etter lov om statlig tilsyn med helsetjenesten § 3), også ga anledning til å pålegge den enkelte virksomhet å føre internkontroll, jf. Ot.prp. nr. 60 (1993-1994), s. 30. Plikten for de enkelte kommunale helsevirksomheter til å føre internkontroll kom med en tilføyelse, gjeldende fra 1. januar 1995: «Det kan også gis regler om plikt til å ha internkontrollsystemer og til å føre internkontroll for å sikre at krav fastsatt i eller i medhold av denne lov overholdes.» kommunehelsetjenesteloven § 4a-1.

[277] «Departementet har merket seg at enkelte av høringsinstansene frykter habilitetskonflikter når kommunen både opptrer som barnehageeier og tilsynsmyndighet. Departementet har imidlertid tro på at kommunene er seg sine roller bevisst.» Ot.prp. nr. 72 (2004-2005), s. 73.

[278] Det understrekes at et pålegg fra departementet om internkontroll for «den faglige styringen med direktoratets myndighetsutøvelse og tjenesteyting» vil være noe annet enn virksomhetsstyringen i medhold av økonomistyringsreglementet. NOU 2006:14, s. 90.

[279] At dette kan være problematisk er så vidt berørt, «et særlig punkt er å sikre tilsynsaktiviteten den nødvendige uavhengighet i forhold til direktoratets virksomhet.» Det nærmeste utredningen kommer en anvisning på hvordan uavhengighetskonstruksjonen skal sikres, synes å være en stor tiltro til at den oppnås gjennom de egenskaper internkontroll har som *metode*: «I tillegg kreves rollebevissthet, høy tilsynsfaglig kompetanse og metodiske ferdigheter.» NOU 2006:14, s. 93.

sideeffekter. Forsvarlighet, rettssikkerhet og individers rettighetsvern er neppe det eneste som vil være på agendaen i den faglige styringen. I innledningen til delrapport 2 fremgår det at de foreslåtte tiltakene også skal sikre direktoratets politiske lydhørhet.[280] Faren ved et styringssystem der den politiske lydhørheten gjøres til gjenstand for jevnlig systemkontroll og bearbeiding gjennom sykliske forbedringsprosesser, er at departementets politiske rolle kan bli uklar. Med et internkontrollsystem som verktøy for at direktoratet skal internalisere politiske føringer, kan politisk overstyring både tilsiktet og utilsiktet bli kamuflert som faglige forbedringer. En eventuell politisk overstyring bør av transparenshensyn fremstå som nettopp det, og ikke se ut som noe direktoratet selv har «lært seg» gjennom sitt eget internkontrollsystem.

4.4.5 Internkontrollpliktbrudd og foretaksstraff

Lovverket inneholder altså mange plikter til internkontroll, og det er et svært høyt antall virksomheter som er underlagt en eller flere av disse bestemmelsene. Tar man dette i betraktning, er det svært sjelden saker om brudd på internkontrollplikter kommer opp for domstolene. Mye av forklaringen ligger antakelig nettopp i at det er særskilte tilsynsorganer som har kontroll med virksomhetenes internkontroll som oppgave. Selv der internkontrollplikten er understreket av straffesanksjoner fører dette i praksis sjelden til saker for domstolene.

Straffelovens regler om foretaksstraff, kapittel 3a som ble tatt inn i loven i 1991, brakte internkontroll et stykke nærmere rettssalene.[281] Ileggelse av foretaksstraff krever ikke identifiserbarhet eller entydig årsaksforhold, det kan også anvendes ved anonyme og kumulative feil.[282] Selv om internkontroll ikke er nevnt konkret i disse bestemmelsene, har manglende internkontroll vært vurdert som et hensyn i enkelte avgjørelser om foretaksstraff.

At en virksomhet kan straffes for manglende eller mangelfulle internkontrollsystemer er stadfestet ved dom i Høyesterett.[283] Saken gjaldt en arbeidsulykke. En arbeidstaker falt ned under oppheising av takplater på et nybygg, og ble lettere skadet. Selskapet ble funnet å ha forsømt å gi arbeidstakere på nybygget den opplæring, øvelse og instruksjon som var nødvendig. Høyesterett uttalte også at det «ved forskrifter gitt i medhold av arbeidsmiljøloven § 16a

[280] NOU 2006:14, s. 55.
[281] «Når et straffebud er overtrådt av noen som har handlet på vegne av et foretak, kan foretaket straffes.» straffeloven [1902] § 48a første punktum. Å handle på vegne av foretaket innebærer en terskel for hvor illojale medarbeidere som kan utløse denne typen straff mot foretaket.
[282] Et av de særlige hensyn for avgjørelse og utmåling som det kan legges vekt på, der internkontrollsystemet kan ha vekt som bevis, er «om foretaket ved retningslinjer, instruksjon, opplæring, kontroll eller andre tiltak kunne ha forebygget overtredelsen.» straffeloven [1902] § 48b(c).
[283] Rt. 1995 s. 278.

er påbudt at det i bedriftene skal sørges for internkontrollsystemer for å fremme arbeidsmiljø og sikkerhet for vern mot helseskade. Selskapet er dømt for ikke å ha etterlevet dette påbudet.» Selskapet ble ilagt foretaksstraff på kr. 50.000, et beløp som var dobbelt så høyt som i domsslutningen fra herredsretten. Begrunnelsen for dette lød «særlig i betraktning av den risiko i arbeidssituasjonen som selskapet har forsømt å forebygge, finner jeg at boten er satt for lavt, og at aktors påstand er passende.»

Også manglende etterlevelse av plikt til internkontroll etter forurensningsloven har vært oppe i Høyesterett, i en sak om ammoniakkutslipp.[284] Under arbeidet med å montere et nytt og utvidet kjøleanlegg, ble det oppdaget at vann hadde trengt inn i systemet slik at ammoniakken måtte tappes ut. En ansatt i en bedrift som driver installasjon og service av kjøleanlegg, helte ut ammoniakken slik at den fulgte overvannsnettet ut i Sandvikselven. All fisk i elven nedenfor utslippsstedet døde. Etter å ha etterforsket forholdet, utferdiget politiet et forelegg mot bedriften, for tre overtredelser mot forurensningsloven. Foreleggets post I gjaldt selve utslippet, post II unnlatt avfallslevering, og post III manglende internkontroll. Forelegget ble ikke vedtatt, og gikk derfor til pådømmelse i retten.

Et sentralt spørsmål i dommen var kriteriet i straffeloven § 48a om den ansatte handlet på vegne av bedriften, til tross for en viss grad av illojalitet mot muntlig instruks. Retten fant at handlingen likevel skjedde på vegne av bedriften, og har i den forbindelse blant annet lagt vekt på at bedriften «manglet retningslinjer og opplæringstiltak om vannholdig ammoniakk som kunne ha forebygget overtredelsen.» I internkontrollterminologi kan dette oversettes til manglende beslutninger om og iverksetting av risikoreduserende tiltak. Bedriften ble dømt til å betale foretaksstraff både for brudd på tiltalens post I (selve utslippet) og post III (manglende internkontroll). Førstvoterende «anser også den manglende internkontrollen for å representere en alvorlig lovovertredelse – det foreligger omfattende brudd på foretakets plikter etter internkontrollforskriften.» Botens størrelse ble fastsatt til 1,2 millioner kroner.

I den relativt sparsomme rettspraksisen der internkontrollsystemer har vært en del av bevissituasjonen, har vurderingen stort sett vært begrenset til et spørsmål om hvorvidt internkontrollsystemet er på plass i virksomheten eller ikke. Domstolene har så langt ikke gått inn i detaljerte vurderinger av det slag som tilsynsorganene gjør i en systemrevisjon. Man kan si at det elementet i idealtypen som først og fremst blir understreket gjennom disse eksemplene fra rettspraksis er aktivitetsplikten.

[284] Rt. 2007 s. 1684.

4.4.6 Resultatene av eksterne tilsyn

Resultater av eksterne tilsyn finnes på to nivåer. Det ene nivået er det håndfaste resultatet fra tilsynet med den enkelte virksomhet, det andre nivået er tilsynsvirksomhetens samlede effekt på samfunnshensynet.

Resultater på det første nivået er i de fleste tilfeller en rapport, som beskriver funn og vurderinger hos det enkelte tilsynsobjekt. En slik rapport har mye til felles med en revisjonsberetning. Vurderingene aggregeres opp til en samlet karakter, og den enkelte vurdering kan også inneholde forslag til forbedringer. Noe varierende med de ulike tilsynsorganers sanksjonshjemler, kultur og praksis, og etter hvor graverende funnene er, gis det av og til også pålegg om utbedringer. Politianmeldelse for straffbare handlinger er også et mulig utfall av et tilsyn, men det vil være svært sjelden, og et stort skritt ut av den kontinuitetsfremmende tilsynsformen risikobasert internkontroll er ment å være.

Tilsynsorganet redegjør for resultater på det andre nivået, effektene for samfunnshensynet, overfor offentligheten og sine overordnede i statsforvaltningen. En slik redegjørelse gis ofte i form av årsmeldinger eller lignende. Mellom disse to resultatnivåene, hensynet til kontinuitet og velfungerende internkontrollprosesser eller hensynet til samfunnshensynet totalt sett og tilliten til den offentlige kontroll, ligger det noen dilemmaer.

Et av dilemmaene er reaksjon eller ikke-reaksjon på avvik som ligger utenfor besluttet aksept av risiko. Både for den organisatoriske læringen og for effekten på samfunnshensynet er det i mange sammenhenger uhensiktsmessig å legge opp til sterkere reaksjoner enn at avviket påpekes. Påpekningen gir virksomheten mulighet til selv å korrigere på den måten de med sin nærhet til problemet vet vil være den beste. Tilsynsorganet inntar skriftefaderens rolle, og utøver en form for ulovfestet absolusjonskompetanse. Det ytre resultat er gjerne en virksomhet som lover bot og bedring. Det er grunn til å anta at allmennhetens tillit til svake reaksjoner kan være skjør, slik at mange alvorlige avvik innen et område på sikt vil føre til innskjerpinger i virksomhetenes handlingsrom.

Et annet dilemma er at tilsynsorganet må innta risikoskapers perspektiv, for å forstå og vurdere virksomhetens internkontrollsystem, og risikobærerens perspektiv som talsmann for samfunnshensynet. Internkontrollmetodikken gir ikke rom for å innta en helt entydig rolle som ombud eller stedfortreder for risikobæreren. Tilsynsorganet må, i større grad jo nærmere idealtypen det aktuelle regelverket ligger, forene to motstridende hensyn. Virksomhetenes handlingsrom skal respekteres så langt som mulig, samtidig som samfunnshensynet skal ivaretas best mulig. Det er denne balansen som er resultatene av eksterne tilsyn. For å oppnå

god balanse trenger tilsynsorganet både faglig autoritet inn mot virksomhetene og en form for karismatisk autoritet, eller i det minste en viss troverdighet som ombud for samfunnshensynet, overfor risikobærerne og samfunnet ellers.

4.5 Reguleringsmetodens effekter og egnethet

Om resultatene av eksternt tilsyn med internkontroll kan være vanskelig å gjøre klart rede for, er det ikke mindre komplisert å ta stilling til metodens effekter og egnethet for å regulere de ulike samfunnshensynene totalt sett.[285] Hensikten her er imidlertid ikke å «felle dom» over en reguleringsmetode. Formålet er først og fremst å gi bakgrunn for påstander om et komplekst samspill mellom ulike typer og nivåer av regler i den reguleringen som er utgangspunkt for avhandlingens problemstilling. Disse betraktningene om effekter og egnethet er verken fullstendige eller konkluderende, men tar sikte på å synliggjøre enkelte fordeler og dilemmaer ved risikobasert internkontroll.

4.5.1 Motsetninger mellom samfunnshensyn og egeninteresser

Det idealtypiske utgangspunkt, full suverenitet for virksomhetene, har stått relativt sterkt selv om det innen alle konkrete plikter til internkontroll finnes reelle begrensinger i handlingsrommet. Det er imidlertid noen tegn til at utviklingen kan gå i retning av større formelle innskrenkninger i virksomhetenes handlingsrom. En innvending som hele tiden har vært på agendaen er spørsmålet om konflikt eller harmoni mellom virksomheters egeninteresser og samfunnshensynet. Særlig på de områdene der risikobærer ikke er representert, og vanskelig kan gjøre sin stemme hørt, kan det være vanskelig å skape den nødvendige tilliten til at en virksomhet bruker sitt handlingsrom på en måte som faktisk ivaretar samfunnshensynet godt nok.[286]

---

[285] At metoden i seg selv er vanskelig evaluerbar er treffende beskrevet i Power (2004), s. 49: «Although an internal control revolution lies at the heart of the risk management explosion, process-based risk management and internal control systems suffer inherently from the problem of demonstrating their own effectiveness, despite upbeat claims and continuing attempts to recast control activity as a value proposition.»

[286] I et foredrag om miljørett ved 36. nordiske juristmøte uttrykkes en reservasjon av dette slaget: «Bruken av internkontrollsystemer bygger dels på at bedriften selv er nærmest til å holde oppsikt med at den følger de fastsatte krav, og på at internkontroll kan være et middel til å internalisere miljøkravene i bedriftskulturen, dels på at offentlige myndigheter har begrenset kapasitet til å føre kontroll. Men faren for egeninteresse gjør at internkontroll aldri må bli enerådende, og bør tilsi åpenhet om internkontrollen i forhold til den miljøinteresserte allmennhet.» Inge Lorange Backer (2002): «Miljöskydd och ekonomiskt utnyttjande – principen om hållbar utveckling». I: *Förhandlingarna vid det 36. nordiska juristmötet i Helsingfors 15.-17. augusti 2002*, s. 113–141.

Faren for egeninteresse, at handlingsrommet i det idealtypiske internkontrollsystemet misbrukes til ikke å synliggjøre og motvirke trusler mot samfunnshensynet, er en tungtveiende innvending. Interessenter, enten det er den miljøinteresserte allmennhet, fagforeninger, leverandørnæringer, restaurantgjester eller andre, er ikke direkte representert i et internkontrollsystem. Det er nærliggende å prøve å bøte på dette ved å tolke et statlig tilsynsorgan som en indirekte interesserepresentant. En slik tolkning har imidlertid også svakheter. Tilsynsorganene har normalt ansvar for et avgrenset samfunnshensyn, mens hver interessent eller interessentgruppe vil ha forskjellige syn på hvordan ulike samfunnshensyn bør avveies mot hverandre.[287]

Å betrakte tilsynsorganet som en indirekte interesserepresentant er også problematisk fordi tilsynsmetodene, forvaltningslovens saksbehandlingsregler, og forutsetningen om å respektere det handlingsrommet virksomheten har som følge av reguleringsmetoden, gir tilsynsorganet begrensete muligheter til direkte overprøving av noe som eventuelt kan oppfattes som virksomhetens egeninteresse. Datatilsynets egen presentasjon av sitt oppdrag, som både en tilsyns- og en ombudsrolle, illustrerer dilemmaet.[288] Som ombud kan de veilede den enkelte registrerte, som er bekymret for sitt eget personopplysningsvern, om hvordan de best kan ivareta sine interesser overfor den behandlingsansvarlige virksomheten. I tilsynsrollen, derimot, må Datatilsynet se på de helhetlige vurderingene virksomheten har gjort, og være lydhøre for argumentasjonen bak valg, beslutninger, iverksetting og avvikshåndtering. Tilsynsrollen har sin egen logikk, som bør holdes atskilt fra tilsynsorganets råd og bistand til andre interessenter.

4.5.2 Motsetninger mellom rettigheter og risikohåndtering

En annen regulatorisk trend, som kanskje høster mer rettsvitenskapelig oppmerksomhet enn risikobasert internkontroll som reguleringsmetode, er en antatt tiltagende rettighetsorientering. «Antatt» er her et mildt forbehold, fordi det på samme måte som når man skal påvise internkontrollmetodikkens fremvekst er tilsvarende metodeproblemer med å dekomponere en

[287] Innen interessentteori problematiseres det forhold at samme person inngår i ulike interessentgrupper, og derfor ikke nødvendigvis har entydige interesser overfor samme virksomhet. Dirk Matten og Andrew Crane (2005): «What is stakeholder democracy? Perspectives and issues». I: *Business Ethics: A European Review,* s. 6–13.

[288] Jf. egenomtale på nettsiden: «Datatilsynet er et tilsyn og et ombud for personvern i Norge», Datatilsynet, «Om Datatilsynet – Datatilsynets oppgaver»: *http://www.datatilsynet.no/templates/Page____954.aspx*.

rettsutvikling slik at det gir en egnet beskrivelse av rettighetsorienteringens omfang. Rettighetsorienteringens viktigste uttrykk de senere år er menneskerettsloven.[289]

På andre, mer sektoravgrensede områder er det også økende bruk av rettighetsbegreper i lovgivningen. Pasientrettigheter har gitt navn til en egen lov, ellers er målsetninger i lovgivningen i en del sammenhenger utformet som rettigheter, slik som rett til barnehageplass, rett til fritt sykehusvalg, rett til miljøinformasjon og så videre. Det er ikke uten videre gitt at en rettighet legges til grunn som mer tungtveiende enn om samme norm hadde vært formulert som en pliktregel for den som skal oppfylle rettigheten. Å formulere regler i en rettighetsdrakt kan kanskje av og til i like stor grad være valg av en kommunikasjonsform som en reell vektlegging av rettighetssiden. Samtidig er rettighetsformuleringer brukt forholdsvis edruelig, det er ikke alle slags regler som kan formuleres som rettigheter på en hensiktsmessig måte. En persons rett til ikke å bli kjørt ned av en påvirket bilist ville nok kommunisere dårligere enn et forbud mot å kjøre bil i påvirket tilstand. Spørsmålet her gjelder imidlertid ikke rettighetsorienteringens omfang, men i hvilken grad risikobasert internkontroll står i motsetning til en rettighetsorientering.

Et idealtypisk internkontrollsystem kan sies å stå i en utilitaristisk tradisjon. Regnestykkene over nytte gjøres på et akkumulert nivå, avveiningene mellom rasjonell drift og samfunnshensyn er systemvurderinger, små avvik blir rettferdiggjort av den overordnede balansen.[290] Den utilitaristiske rettferdiggjøringen av virksomhet som innebærer en risiko er at det moralsk kritikkverdige tynnes ut ved redusert sannsynlighet for skade, mens nytteverdien ved virksomheten er konstant.

Rettighetsorientering er en motsats til dette. En ofte sitert formulering er rettsfilosofen Ronald Dworkins beskrivelse av rettigheter som «politiske trumfkort på individets hånd».[291] Disse motsatsene kan sameksistere på ulike vis. En måte er ikke-berøring. Det ville forutsette at rettigheter og risikobasert internkontroll regulerer atskilte deler av virkeligheten. Slik kan det være et stykke på vei, men innen alle kategoriene av samfunnshensyn som reguleres

[289] Menneskerettsloven, 21. mai 1999 nr. 30. Konvensjonenes forrang ved motstrid og overnasjonale domstolers inntog har satt spor, både i rettsdogmatikken og i politisk debatt. Denne utviklingen har også møtt motforestillinger, blant annet i Makt- og demokratiutredningens sluttbok, Øyvind Østerud m. fl. (2003): *Makten og demokratiet: en sluttbok fra Makt- og demokratiutredningen*.

[290] I en artikkel om det moralfilosofiske grunnlaget for regulering av risiko, knyttes det utilitaristiske perspektivet til et fortynningsproblem ved beregning av risiko: «Det är förbjudet för mig att köra ihjäl en fotgängare. Det torde också vara förbjudet att köra på ett sådant sätt att sannolikheten är 1 på 10 att köra ihjäl en fotgängare. Men det är alldeles uppenbart inte förbjudet att köra på ett sådant sätt att sannolikheten är 1 på 1000000000 att köra ihjäl en fotgängare – i så fall skulle det vara förbjudet att köra bil överhuvudtaget. Var drar vi gränsen, och varför?» Sven Ove Hansson (2002): «Kan moralfilosofin hantera riskproblemen?». I: *Osäkerhetens horisonter. Kulturella och etiska perspektiv på samhällets riskfrågor* s. 53–67. (s. 54).

[291] Fra hans bok *Taking Rights Seriously* (1977). Her er det sitert slik det er oversatt i NOU 1999:27, s. 20.

gjennom internkontroll finnes det områder hvor risikoskaper og risikobærer har forskjellige interesser. En annen måte å sameksistere på er å utvikle kjøreregler, eller motstridsnormer. Slike normer utvikles gjerne gjennom rettspraksis. I prinsippet kan de nok også utvikles på avgrensete områder gjennom tilsynsorganenes praksis, men ettersom tilsynsvirksomheten hovedsakelig er basert på systemrevisjon, og de rettighetene som hevdes sjelden er ufravikelige, er det grunn til å anta at risikoskapers handlingsrom som oftest blir premissgivende. En tredje måte er laissez-faire sameksistens. Ved ikke å velge noen bevisst strategi for å håndtere motsetningene, kan det foregå en gjensidig påvirkning som ikke er direkte styrt, men der utilitaristiske kalkyler og rettigheter får prøve å måle krefter, og resultatet bli som det blir.[292]

I rettsteori finner man argumenter både for å styrke rettigheter, som et proporsjonalt mottiltak til den sterkere samfunnsstyringen som risikoorienteringen er et uttrykk for, og for sterkere kontroll med risikoskapers egne prosesser for å ivareta samfunnshensynet.[293] Et interessant argument *mot* rettighetsorientering, på de områdene som er gjenstand for ønsket eller legitim aktivitet som medfører risiko, er at regelverk som uttrykker noens rettigheter vil mangle et tilstrekkelig vern mot utelatelser.[294] Om en konkret rettighet er ivaretatt er bare oppe til prøve når noen gjør den gjeldende, ofte etter at en noe man ønsket å unngå har inntruffet. Det idealtypiske internkontrollsystemets aktivitetsplikt gir et bedre svar på problemet med utelatelser enn en rettighetsteori tilbyr. På den annen side gir rettigheter et bedre vern mot en virksomhets bruk eller eventuelle misbruk av sitt handlingsrom til å nedprioritere individers rettigheter til fordel for balansen i det aggregerte nytteregnskapet.

På et prinsipielt plan finnes det altså visse grunnleggende motsetninger mellom idealtypen risikobasert internkontroll og en rettighetsorientering, selv om internkontroll også kan og bør være et verktøy for å ivareta risikobæreres interesser. Den prinsipielle motsetningen betyr imidlertid ikke nødvendigvis at resultatene ikke er *rettferdige*. Rettsfilosofen John Rawls beskriver flere alternative innfallsvinkler til rettferdighet. Dersom man står uten et uavhengig kriterium for å vurdere om en avgjørelse er rettferdig, kan en rettferdig prosess være en måte å skape rettferdige avgjørelser på. Hans enkle eksempel er to barn som skal dele et kakestykke:

---

[292] En aksept for ulike reguleringsmetoder som lever side om side kan betegnes som *rettlig pluralisme*, selv om det er litt risikabelt fordi pluralismebegrepet brukes på mange måter. Et pluralismebegrep som også omfatter risikobasert internkontroll i tråd med idealtypen her, er godt beskrevet i Christine Parker (2008): «The Pluralization of Regulation». I: *Theoretical Inquiries in Law,* s. 349–369.

[293] Barbara Hudson (2001): «Human Rights, Public Safety and the Probation Service: Defending Justice in the Risk Society». I: *The Howard Journal,* s. 103–113.

[294] «A rights theory might absolutely prohibit actions when the actor directly intends to expose other individuals to risk, but not those where risk is only a side-effect or further consequence. The second differentiates positive actions from negative actions or omissions. A rights theory might construct absolute rules concerning harm caused by positive acts, but not those resulting from omissions.» Schroeder (1986), s. 526.

En prosess der den ene deler stykket i to, og den andre får velge først, gir et resultat man kan anerkjenne som rettferdig. For Rawls er slik prosessuell rettferdighet ikke ideelt, men en slags utvei i tilfeller der man mangler et egnet vurderingskriterium. Han ser det som problematisk at ingenting kan bedømmes som rettferdig eller urettferdig før prosedyren faktisk er utført.[295]

Idealtypisk internkontroll, særlig når den er anvendt på samfunnshensyn av kategorien individers rettighetsvern, heller mer mot å være en prosessuell metode for rettferdighet enn en rettighetsorientering. Aktivitetsplikten er det som sikrer at prosedyren faktisk gjennomføres. Innvendingene mot at resultatene av internkontroll skal måtte aksepteres som rettferdige er imidlertid fremdeles til stede. Det vil ofte være en maktskjevhet mellom risikoskaper og risikobærer. Utformingen av prosedyrene skjer, og skal skje, på virksomhetens premisser.

4.5.3 Sementering av virksomhetsgrenser

Risikobasert internkontroll er en reguleringsmetode som er designet primært for å sikre det angitte hensynet innenfor virksomheten. I tillegg har slike bestemmelser lagt vekt på å sikre vertikal integrasjon.[296] En virksomhet som er underlagt en eller flere plikter til internkontroll kommer ikke unna sitt ansvar for samfunnshensynet gjennom å stykke opp virksomheten eller å utkontraktere oppdrag.

Ved horisontalt samarbeid mellom virksomheter er det sjelden noen direkte plikt til, og i praksis ofte heller ikke mulig å oppnå, felles mål og kriterier for aksept av risiko. En adgang til horisontalt samarbeid, der det ikke er noen underordningsrelasjon mellom virksomhetene, innebærer ikke at den ene virksomheten nødvendigvis vil være bundet av hvor godt eller dårlig den andre virksomheten ivaretar samfunnshensynet. Mens en virksomhet som utkontrakterer sin egen behandling av personopplysninger beholder det fulle ansvaret i den vertikale relasjonen til databehandler, vil en berettiget utlevering av opplysningene til en annen virksomhet, som da selv blir ansvarlig for sin egen behandling av disse opplysningene, ikke innebære noen plikt til å forsikre seg om at mottakende virksomhets internkontrollsystem fungerer og sikrer den registrertes personvern i tilstrekkelig grad.[297]

---

[295] «A distinctive feature of pure procedural justice is that the procedure for determining the just result must actually be carried out; for in these cases there is no independent criterion by reference to which a definite outcome can be known to be just.» John Rawls (1999): *A Theory of Justice*, s. 75.

[296] Vertikal integrasjon har vært sentralt i mange slike regelverk, helt siden starten med Oljedirektoratets retningslinjer [1979], der rettighetshaver er ansvarlig for at enhver som utfører arbeid for ham, uansett om vedkommende er ansatt, kontraktør eller underkontraktør, overholder bestemmelsene.

[297] Personopplysningsforskriften § 2-15, pålegger riktignok at det foreligger avtale om sikkerhetstiltakene med de aktørene som er involvert i den elektroniske kommunikasjonen av opplysningene. Bestemmelsen i første ledd: «Den behandlingsansvarlige skal bare overføre personopplysninger elektronisk til den som tilfredsstiller kravene i forskriften her», sikrer strengt tatt bare at mottakende virksomhet skal ha gjennomført tilsvarende

Faren for at samfunnshensynet svekkes ved horisontalt samarbeid kan møtes med ulike strategier. En strategi, som kan være aktuell der grunnlaget for tillit mellom de samhandlende virksomhetene er relativt lavt, er eksterne tredjeparts sertifiseringsordninger. Metodisk sett vil dette ligne et eksternt statlig tilsyn, sertifisering av virksomhet er som regel basert på en systemrevisjon med virksomhetens egne kontrollprosesser. En viktig forskjell er at en positiv bekreftelse kan skaffes, henges opp på veggen, eller forevises samarbeidsparter. Med statlig tilsyn vil det være vanskelig å få en periodisk oppdatert bekreftelse på at samfunnshensynet ivaretas. Fravær av pålegg og kritiske merknader har begrenset verdi som dokumentasjon av etterlevelse.

En annen strategi for å hindre at horisontalt samarbeid svekker samfunnshensynet er å utforme reguleringen mer detaljert. Større detaljnivå har som kostnad at virksomhetenes handlingsrom innskrenkes. En beslektet strategi er at virksomhetene innen en bransje kan velge en selvpålagt reduksjon av fleksibiliteten gjennom tekniske standarder eller bransjenormer, der de forplikter seg til felles standarder for aksept av risiko. Et eksempel på dette er bransjenormen for informasjonssikkerhet for alle virksomheter som vil kobler seg til Norsk helsenett.[298] En tredje strategi, som ville være å bevege seg noe mer bort fra idealtypen risikobasert internkontroll, er å legge om reguleringen slik at den baseres på virksomhetseksterne risikovurderinger.[299] Også denne strategien reduserer innslaget av selvregulering.

4.5.4 Internkontrollens betydning for behandling av helseopplysninger

I denne brede gjennomgangen av risikobasert internkontroll er det presentert flere trekk ved denne reguleringsmetoden som kan ha en viss betydning for regulering av og kontroll med behandling av helseopplysninger. Det første er at de virksomhetene som behandler helseopplysninger er underlagt flere forskjellige plikter til internkontroll. De mest sentrale er helseregisterlovens to internkontrollbestemmelser.[300] Det er i særlig grad kravene til informasjonssikkerhet som kan sies å ligge svært nær opp til den konstruerte idealtypen. Internkontroll er imidlertid også et sentralt element i annen regulering, som blant annet dreier seg om

internkontrollprosesser, den gir ingen garanti for at beslutninger om mål, aksept av risiko eller risikoreduserende tiltak faktisk gir et harmonisert sikkerhetsnivå som resultat.

[298] Sikkerhetsnormen. En fyldigere presentasjon av denne normen følger nedenfor i kapittel 6.2.4.2. Det felles, harmoniserte nivået for akseptabel risiko er likevel ikke mer detaljert enn at det fremdeles overlater betydelig operasjonalisering og fastlegging av risikoreduserende tiltak til den enkelte virksomhet.

[299] Dette ville være beslektet med utviklingen innenfor hensynet samfunnssikkerhet, og innebære en omlegging til en annen og mindre autonom variant av internkontrollprinsippet, jf. trendene beskrevet i kapitlene 4.2.3 og 4.2.4. Antakelig innebærer dette en større omlegging av reguleringen enn de øvrige strategiene.

[300] Helseregisterloven, § 16 om informasjonssikkerhet og § 17 om å oppfylle krav i eller i medhold av loven.

virksomhetenes tiltak for å sikre forsvarlighet og pasientsikkerhet. Internkontrollaktivitetene er dermed noe som omfatter nærmest alle sider ved virksomheten.

Det andre trekket er at de grunnleggende behovene som motiverer denne reguleringsmetoden, behovene for fleksibilitet fordi virksomhetene er relativt forskjellige, kontinuitet fordi de ikke kan unnværes, og vertikal kontroll fordi styrings- og underordningsrelasjonene er kompliserte, gjør seg sterkt gjeldende. En høy grad av selvregulering er kanskje derfor det beste og sunneste for helsesektoren totalt sett, men det er likevel grunn til å være bekymret for om det er forsvarlig å legge opp til økt bruk av helseopplysninger på tvers av IT-systemer og organisatoriske grenser uten å harmonisere sikkerhetsnivået i en slik grad at det reduserer den enkelte virksomhets handlingsrom.

Det tredje trekket ved reguleringsmetoden, som er viktig i denne sammenhengen, er at virksomhetenes selvregulering inngår i et samspill med andre, og ofte mer konkret utformede, regler. Å forstå internkontrollpliktene er i en del sammenhenger nødvendig for en holdbar forståelse av den samlede reguleringen. Internkontrollsystemene, som i tillegg til virksomhetens egne tiltak for oppfølging og kontroll også uttrykker virksomhetens egen normsetting innen gitte rammer, er en betydelig del av det landskapet som hele den komplekse reguleringen av tilgang til og videreformidling av helseopplysninger inngår i.

Del II:

Behandling og beskyttelse av helseopplysninger

5 Helseopplysninger og informasjonssystemer

Dette kapitlet begynner med noen betraktninger om hva helseopplysninger er, hvordan de blir til, og hvilket forhold de har til den bakenforliggende virkeligheten. Dernest følger en liten oversikt over noen typer systemer og prosesser for behandling av helseopplysninger. Både forskjeller i opplysningenes form og forskjeller mellom hva slags informasjonssystemer de behandles i, og av hvilke aktører, har betydning for hvordan tilgang og videreformidling kan eller bør reguleres og kontrolleres.

5.1 Helseopplysninger og virkeligheten

Begrepet helseopplysning er, som nevnt innledningsvis i avhandlingen, legaldefinert i helseregisterloven.[301] I denne drøftingen er det imidlertid behov for noen flere nyanser enn å kvalifisere hva som ligger innenfor eller utenfor begrepet. Perspektivet her er at helseopplysninger er produserte beskrivelser eller representasjoner av noe som har med pasientens helse å gjøre. Dette «noe» omfatter blant annet hvordan pasienten har det og hvordan han fungerer, den medisinske vurderingen av pasientens tilstand og behov, prøveresultater, behandlingstiltak og behandlingsresultater, og beslutninger om og administrasjon av vurderingene og tiltakene.[302]

[301] Helseregisterloven § 2(1)(1).

[302] Diagnosen er kanskje den opplysningstypen som særlig oppfattes som sinnbildet på helseopplysninger, selv om begrepsdefinisjonen er langt videre. Diagnoser er imidlertid godt egnet for å illustrere de bakenforliggende problemene med å kontrollere opplysninger på tvers av organisasjoner, teknologier og kanskje særlig mellom ulike bruksformål. Dette sitatet illustrerer tankekorset: «Ein kvar diagnose er logisk-analytisk sett ein domsslutning. Den er ein domsslutning som er gitt på visse premiss, og som kan fungere ulikt avhengig av ytre samanheng – kontekst – den brukes i. Ein depresjonsdiagnose korrekt brukt klinisk kan redde liv. Men den kan også slå beina under ein pasient, forverre sjølvbiletet og fungere destruktivt. Eit spesielt problem har vi når ein diagnose blir brukt i ein annan kontekst enn det den var tenkt til. Det er til dømes problematisk når den deprimerte, mange år etter at 'lykkepillen' er svelgd unna, oppdagar at han ikkje kan få livsforsikring på ordinære vilkår fordi han har 'feil' diagnose.» John Nessa (2000): «Diagnosar drep – og gjer frisk». I: *Utposten,* s. 4–7. (s. 4).

At en opplysning er produsert, viser til en tilblivelsesprosess som involverer ulike aktører. At opplysninger er beskrivelser og representasjoner, antyder noen forskjellige trekk ved opplysningenes form og innhold. Overskriften *helseopplysninger og virkeligheten* peker på at opplysningene ikke «er» virkeligheten, men formidler kunnskap om en avgrenset del av den. En opplysning kan sjelden betraktes som et helt umiddelbart og entydig uttrykk for det den representerer. Opplysningene har oftest form av standardiserte vendinger og koder som det er faglig konsensus om. I en viss forstand kan det være mer presist å si at opplysningene representerer instanser av denne faglige konsensusen, anvendt i partikulære situasjoner. Det er et slags filter mellom det opplysningene representerer, og ting som foregår i eller gjøres med pasienten. Ordet virkelighet kunne derfor kanskje ha vært satt i anførselstegn. For denne avhandlingens formål er det imidlertid ikke nødvendig å være fullt så pirkete.

5.1.1 Helseopplysningers tilblivelse og form

Mange helseopplysninger oppstår først i muntlig form. Pasienten beretter om et symptom, legen sier noe om hva det kan skyldes og hva som bør gjøres. Selv i en helt og holdent muntlig situasjon gjelder visse normer for hvem som kan fortelle hva videre, til hvem, og under hvilke betingelser. Selv om det er en klar sammenheng mellom normene for muntlig formidling av opplysninger og formidling av dokumentasjon, taushetsplikten omfatter begge deler, er det i denne fremstillingen valgt å sette som startpunkt at helseopplysningene oppstår i og med helsepersonells dokumentasjonsplikt.[303] Dokumentasjonsplikten har en lang historie, og har hele tiden hatt et element av å skulle sikre kontrollmyndigheters mulighet for å etterprøve at virksomheten er forsvarlig.[304] Som følge av arbeidet med å få kontroll over epidemiske sykdommer fikk leger også plikt til å rapportere til helsemyndighetene om pasienter de behandlet for slike sykdommer.[305] Rapporteringsplikter på individnivå, alternativt betegnet som meldeplikter, finnes i dag på flere områder.[306] Dokumentasjons- og rapporteringsplikter

[303] Helsepersonelloven § 39 første punktum: «Den som yter helsehjelp, skal nedtegne eller registrere opplysninger som nevnt i § 40 i en journal for den enkelte pasient.»
[304] Et tidlig eksempel, antakelig landets første lovbestemte plikt til å nedtegne enkeltpasienters tilstand, finner man i sinnsykeloven [1848], 17. august 1848, (Opphevet) § 5. Pasientens fulle navn, alder, fødested med videre skulle nedtegnes i en «Personalprotocol», det samme skulle «nøiagtig Beskrivelse over Patientens Legems- og Sjels-Tilstand og senere de Forandringer, som deri maatte indtræde.» Videre skulle blant annet tilfeller av «Indespærren i eensomt Værelse og mekaniske Tvangsmidler» føres i en «Behandlingsprotocol». Begge protokoller skulle «fremlægges ved hver Visitation af Controlcommissairerne».
[305] Sundhedsloven [1860], 16. mai 1860, (Opphevet) § 20. Legen skulle innberette tilfellet til den lokale sunnhetskommisjon, som skulle berette videre om sykdommen og dens gang til Medicinalbestyrelsen.
[306] Et eksempel som innholdsmessig ligger nær det foregående er smittevernloven, 5. august 1994 nr. 55 § 2-3 første punktum: «En lege som oppdager en smittet person, har meldingsplikt etter forskrifter gitt i medhold av

normerer og formaliserer det å produsere helseopplysninger. Pliktene bidrar til å sikre at opplysningene produseres. Pliktene bidrar også delvis, men foreløpig i relativt beskjeden utstrekning, til å standardisere form og kommunikasjonsmåte.[307]

Grunnen til å nedtegne opplysninger er imidlertid ikke bare, kanskje heller ikke først og fremst, å oppfylle en lovbestemt plikt. Å skrive ned hva pasienten har sagt, hvilke vurderinger man gjør som behandler, og hvilke tiltak som er eller kan være aktuelle, er en ofte nødvendig støtte for hukommelsen. Helsepersonellet skriver for å lese det selv senere, hvis og når pasienten kommer tilbake. Dernest brukes opplysningene i samarbeidet med annet helsepersonell i behandlingen av pasienten. Opplysningene skrives med det for øye at annet helsepersonell skal lese det de har behov for i dette samarbeidet. Det medfører et krav til at opplysningene er forståelige og meningsfulle innen det fagfellesskapet som skal bruke dem.

Når helsepersonell skriver dokumentasjon, er det i utgangspunktet en nedtegning av hva de gjør i sine faglige aktiviteter. Legen hører på det pasienten sier, og skriver det som anses relevant. Det videre arbeidet kan være å stille diagnose, utføre eller bestille laboratorieprøver, utføre medikamentell eller annen behandling, henvise til annen helsehjelp. Disse aktivitetene er i sin tur opphav til flere helseopplysninger som igjen skal dokumenteres. Også andre grupper helsepersonell har plikt til å dokumentere helsehjelp, for eksempel sykepleievaktens observasjon og behandlingstiltak overfor pasienter på en post, for rett oppfølging fra vaktskifte til vaktskifte.[308]

5.1.1.1 Fri tekst versus formaliserte kodeverk

De ulike formene for dokumentasjon av faglige aktiviteter har vært skrevet og skrives fremdeles i stor utstrekning som prosa. Den som dokumenterer velger ordene selv. Betegnelsen som ofte brukes i informatisk sammenheng er «fri tekst», til forskjell fra formaliserte koder eller standardverdier der den som dokumenter velger blant de forhåndsdefinerte kodene eller tekststrengene.[309] Likevel ville det være upresist å si at fri tekst er helt og holdent uformali-

---

fjerde ledd uten hinder av lovbestemt taushetsplikt.» Denne bestemmelsen hjemler flere forskrifter om plikter til å innrapportere nærmere angitte opplysninger til ulike sentrale helseregistre.

[307] Et eksempel er forskriftsfesting av kommunikasjonsmåte, når leger sender krav om direkte økonomisk oppgjør til Helseøkonomiforvaltningen, gjeldende fra 1. januar 2010. Forskrift om elektronisk kommunikasjon (HELFO), 15. oktober 2009 nr. 1287.

[308] Vaktskifterapport har en del steder relativt nylig endret form fra muntlig til skriftlig, noe som også kan ses som et uttrykk for at pleiefellesskap er i endring, jf. Bodil Hansen Blix (2005): ««Korthuset». Sykepleieres erfaringer med elektronisk sykepleiedokumentasjon i egen praksis».

[309] Denne distinksjonen har fulgt med hele veien, fra første elektroniske journalsystem i Norge ble påbegynt i 1967: «Det måtte ganske enkelt treffes et valg med hensyn til hvilke opplysninger som skulle registreres for senere automatisk databehandling, og hvilke som skulle registreres i form av fri tekst.» Per Kolstad og Kjell

sert. Det ligger et stort forråd av faglige begreper, organisatoriske rammer, kunnskaper og erfaringer bak de ordene helsepersonellet velger å skrive.[310] Et utsagn i en journal kan i mange tilfeller bare forstås rett av en som har kunnskaper om de faguttrykk og standardformuleringer som gjerne inngår i denne formen for dokumentasjon.[311] Uansett om dokumentasjonen har form av fri tekst eller av formaliserte koder dreier det seg sjelden om å finne på noe nytt og originalt, men om å innordne det som skal nedtegnes under et rammeverk som kan forstås av ens fagfeller.

Formaliserte kodeverk, eller nomenklatursystemer, har sitt opphav i epidemiologers og statistikeres behov for å kunne gruppere og sammenligne mønstre i større populasjoner.[312] Senere er det etablert forskjellige kodeverk for blant annet diagnoser, prosedyrer og pasienters funksjonsnivå.[313] Den utstrakte medisinske kodingen brukes til en rekke ulike formål, blant annet til statistikk, planlegging, forskning, og administrasjon av finansierings- og refusjonsordninger. Utvikling og vedlikehold av kodeverkene foregår dels i internasjonale fora, og dels i norske og nordiske fora. De mest omfattende, internasjonalt forankrede kodeverkene som brukes i Norge oversettes og tilpasses. Hvilke kodeverk som skal brukes besluttes i fagpolitiske organer.[314] Krav til og forventninger om bruk av detaljerte koder for å dokumentere og rapportere aktiviteter kan ses som et uttrykk for at premissgivende aktører har økt sin innflytelse over helsetjenestens virksomheter.

Det er kanskje den helt åpenbare forskjellen på fri tekst og formaliserte koder som også er den viktigste forskjellen. En opplysning i form av fri tekst kan uttrykkes i et uoverkommelig høyt antall varianter. Samme mening kan sies med forskjellig tekst. Forskjellige meninger kan

---

Nordbye (1971): «Et system for automatisk databehandling av medisinske journaler». I: *Tidsskrift for Den norske lægeforening,* s. 405–409. (s. 406).

[310] Dette er blant annet påpekt som konklusjon i John Rooksby og Stephen Kay (2001): «Clinical narrative and clinical organisation: Properties of radiology reports». I: *Medinfo 2001. Studies in health technology and informatics*, s. 680–684. (s. 684).: «In this paper we have described the infusion of clinical organisation in clinical narrative. … The consequence of this description is a view of clinical narrative not as static 'free text' but active 'structured text'.»

[311] I introduksjonen til en narratologisk studie av journalskrift er dette omtalt som «en spenning mellom *genrens standardiserte sjablonger* og litterære lån på den ene siden og søken etter *det adekvate enkeltuttrykk* på den andre.» Petter Aaslestad (2007): *Pasienten som tekst: fortellerrollen i psykiatriske journaler. Gaustad 1890–1990*, s. 35 (original utheving).

[312] De første formaliserte kategorilistene som ble samordnet internasjonalt var over ulike dødsårsaker, jf. World Health Organization: «History of ICD»: *http://www.who.int/classifications/icd/en/*.

[313] De mest omfattende, som er obligatoriske i en del sammenhenger og brukes i stor utstrekning i Norge, er diagnosekodene i systemet ICD-10, et eget utfyllende kodeverk ICPC-2 for primærhelsetjenesten, og prosedyrekodeverkene NCSP og NCMP. En del andre kodeverk er også i utstrakt bruk, en oversikt over de viktigste som er gjenstand for sentralisert røkt er omtalt på nettsidene til KITH, «Kodeverk og terminologi»: *http://www.kith.no/samfunns oppgaver/kodeverk_og_terminologi*. I denne avhandlingen har konkrete detaljer fra ulike kodeverk lite å si for resonnementene. Det er bare noen av de prinsipielle forskjellene mellom formaliserte koder, og andre former helseopplysninger kan ha, som er gjenstand for drøfting.

[314] Beslutningene treffes av Helsedirektoratet, som formidler dem i brevs form til aktuelle virksomheter.

være uttrykt med samme tekst, kanskje med subtile nyanser som bare kan skjelnes ved å se opplysningen i sammenheng med andre opplysninger. Både likheter og forskjeller mellom to opplysninger uttrykt som fritekst kan være tilsiktede eller utilsiktede. Når opplysninger fra et høyt antall pasienter tas ut av den sammenhengen der de ble produsert, kategoriseres sammen med andre i større populasjoner, og kanskje hentes frem igjen etter lang tid, vil den frie tekstens manglende stringens og entydighet bli et problem.

Ved bruk av formaliserte koder oppnår man en stringent måte å uttrykke opplysningen på, slik at den kan kommuniseres med et stabilt meningsinnhold, på tvers av teknologier for behandling av opplysningene, over organisatoriske og faglige grenser, og i prinsippet også på tvers av språk og kulturer. At opplysningen har et stringent uttrykk betyr imidlertid ikke at all vaghet og usikkerhet er avskaffet. For det første representerer ikke alle kodeverdier nødvendigvis et like presist og avgrenset innhold, enkelte kodeverdier har karakter av restkategori i tilfelle andre koder på rett nivå i hierarkiet ikke passer.[315] For det andre kommer ikke rett kode på plass av seg selv, den er et resultat av en tilordning, basert på fagpersonens tilegnelse og vurdering av kunnskap om pasientens situasjon og behov.[316] Dermed er ikke forskjellene på fri tekst og formaliserte koder så markante på selve dokumentasjonstidspunktet, når helsepersonell skriver eller koder utfall av konsultasjoner, undersøkelser, vurderinger, behandling eller henvisninger. Forskjellene er imidlertid skjult til stede ved senere formidling og bruk av de samme opplysningene, når det som i utgangspunktet kan ha vært til stede av tvil, forbehold, nyanser eller personlige oppfatninger om hva som er rett tilordning av kodene ikke lenger er med på lasset.

Det finnes ulike syn på fordelene og ulempene ved henholdsvis fri tekst og forhåndsdefinerte koder. Fri tekst er en måte å representere kunnskap på som gir rom for at begrepene utvikles av «insidere» eller profesjonsutøvere i de fagmiljøene der de brukes, i en vedvarende diskurs, og gjerne i små skritt. Kodeverk konstrueres og vedlikeholdes utenfor brukssituasjonene, og må revideres med hele kodeverkets indre sammenheng for øye.[317] Ved bruk av fri tekst bidrar variasjonsrikdommen, sammen med et relativt presist men ikke fasttømret fag-

[315] For eksempel har kodeverket ICD-10 fire koder under diagnosen «J45 Astma», én for allergisk astma, én for ikke-allergisk astma, en kode for kombinasjon av tilstander under de to foregående kodene, og en fjerde kode med beskrivelsen «uspesifisert astma».

[316] Dette er i all hovedsak en manuell prosess, der fagpersonen gjør sine vurderinger og selv «oversetter» til de formaliserte kodene som passer best. Det foregår også noe forskning på automatisk tilordning av medisinske koder fra frie tekstelementer, se for eksempel Thomas Brox Røst m. fl. (2006): «Classifying Encounter Notes in the Primary Care Patient Record» (konferanseartikkel).

[317] Det er nærliggende her å trekke en parallell til de to representasjonsstrategiene for rettslige begreper i kapittel 2.2.2, forskjellen mellom rettslige begreper som utledes fra de rettsreglene som de inngår i, og konstruerte rettslige ontologier.

språk, til en gjensidig påvirkning der både enkelttilfeller subsumeres under begrepene, og begrepene enten befestes eller settes på prøve gjennom enkelttilfellene.[318] Dette er prinsipielt annerledes ved bruk av kodeverk. Kodeverkene forvaltes og røktes av aktører som hører til utenfor brukssituasjonene, selv om enkeltpersoner med egnet faglig bakgrunn deltar i godt monn. Forvaltning av kodeverk er prosesser som gir et potensielt større rom for en ytre normering av dokumentasjonen.

5.1.1.2 Strukturering av informasjon etter innholdstyper

Verken fri tekst eller formaliserte koder har i praksis vært brukt som selvstendig kriteriegrunnlag for å beslutte hvem som skal ha tilgang til helseopplysningene, eller hvem som skal ha mulighet for å videreformidle dem. Det er en annen type formalisering av informasjonen enn kodeverk som har fått relativt stor praktisk innflytelse, særlig over kontroll med tilgang til pasientjournaler i spesialisthelsetjenesten. Denne typen formaliseringen går ut på å gruppere journalens dokumenter etter innholdstyper. Ulike grupper helsepersonell kan da gis tilgang til visse typer dokumenter som de produserer eller har behov for å lese i sitt arbeid.

En grunnmodell for en slik inndeling av journalen i forskjellige typer dokumenter, som kan utvides og detaljeres etter behovene i den enkelte institusjon, har fått det klingende navnet Norgesjournalen.[319] Denne inndelingen kan ses som en av flere metoder for å strukturere journalen etter innholdstyper.[320] Struktureringen etter innhold i Norgesjournalen kan neppe betegnes som en rendyrket emneinndeling, den fremstår mer som en hybrid inndeling som dels reflekterer de aktørene som produserer eller bruker opplysningene, dels egenskaper ved innholdet, og dels den teknologien som produserer innholdet.[321] Det finnes ulike syn på hva

[318] Disse betraktningene om kunnskaper representert som fri tekst er til dels hentet fra Gunnar Ellingsen og Eric Monteiro (2003): «Mechanisms for producing a working knowledge: Enacting, orchestrating and organizing». I: *Information and Organization,* s. 203–229. En noe lignende betraktning finner man også i dette sitatet om samvirket mellom diagnoser og den medisinske kunnskapen: «Når legen set ein diagnose, kan vi difor seie at ho samstundes set ein metadiagnose – dvs. at ho innordnar problemet i eit medisinsk kunnskapssystem som konstituerer diagnosane.» Ekeland, s. 13.

[319] Norgesjournalen stammer fra utredningen *Pasientjournalen : innhold, gruppering og arkivering av pasientdokumentasjon i somatiske sykehus.* (1994). Utredningen anbefalte en inndeling i ti hovedgrupper, med varierende antall undergrupper innen hver av dem. (Hovedgruppene er A: Sammenfatninger/epikriser, B: Legejournal, C: Prøvesvar, vev og væsker, D: Organfunksjon, E: Bildediagnostikk, F: Observasjon og behandling, G: Sykepleiedokumentasjon, H: Rapport annet fagpersonell, I: Ekstern korrespondanse, J: Attester/meldinger/erklæringer).

[320] Tre slike prinsipper for å strukturere er omtalt i Torbjørn Nystadnes (2007a): «EPJ Standard del 1: Introduksjon til EPJ standard», s. 25–26 og i NOU 2006:5, s. 73: Den ene er inndeling etter emne, som i Norgesjournalen, den andre er problemorientert (etter diagnose eller tilsvarende), den tredje etter behandlingsprosess.

[321] En betegnelse som muligens beskriver Norgesjournalen og tilsvarende inndelinger mer treffende enn å kalle den emneinndelt, er *kildeorientert* strukturering. «The record discussed here is a so-called 'source-oriented' record, by far the most common means of record keeping. It entails ordering the different sections in the record

slags strukturering av journalinnhold som er best egnet som hjelpemiddel i den medisinske behandlingen.[322] Det som imidlertid er kildeorienteringens største fordel, og kanskje også dens viktigste begrunnelse i det hele tatt, er at den bidrar med en håndterlig oppdeling av innholdet som et stykke på vei egner seg for å knytte innholdstyper til aktørgrupper. Det er dermed en måte å strukturere omfattende journaler i store institusjoner på, som kan brukes som en del av kriteriegrunnlaget for å beslutte hvem som skal ha tilgang til eller kunne videreformidle helseopplysninger.

En kildeorientert strukturering av journaldokumenter innebærer i prinsippet ingen føringer for hvordan kunnskapen representeres. Forskjellige typer opplysninger, både fri tekst og formaliserte koder, samt andre kategorier som for eksempel måleverdier eller digitale bilder, kan leve side om side i et journaldokument. Det er to grunner til at kildeorientert strukturering er interessant i denne sammenhengen. Den ene, som allerede er nevnt ovenfor, er at den kan være egnet for å inngå i virksomhetens tilgangskriterier. Den andre grunnen, som er beslektet med noen av betraktningene om formaliserte koder ovenfor, er at struktureringen som sådan kan utvikles til normerende premisser som forvaltes av myndighetsorganer eller andre premissgivere utenfor de virksomhetene som behandler helseopplysningene.

Ved endringslov 19. juni 2009 nr. 68 ble det vedtatt flere endringer i helseregisterloven og helsepersonelloven, der hensikten var å legge til rette for å kunne bruke helseopplysninger på tvers av virksomheter i større omfang, og på mer betryggende måte.[323] I forarbeider til denne endringsloven finner man klare indikasjoner på at samordnet regulering for å strukturere journalers innhold, på tvers av virksomhetene, kan bli mer aktuelt fremover. Proposisjonen drøftet dette i relativt forsiktige vendinger, i hovedsak presentert som enkelte høringsinstansers syn som departementet sier seg enig i.[324]

Lovendringen var gjenstand for omfattende debatt i Stortingets helse og omsorgskomité, der både tilhengere og motstandere av lovendringene uttrykte klar bekymring for om helsevesenet er tilstrekkelig rustet for å beskytte opplysningene godt nok over virksomhetsgrenser.

---

according to the different institutional sources the data are derived from: nursing notes, doctors' notes, laboratory results, bacteriology reports, consultations of different specialties, and so forth.» Berg og Bowker (1997), s. 526.

[322] En motsats til kildeorientert strukturering er den *problemorienterte* journalen, der pasientens «problemliste» fungerer som en innholdsfortegnelse til ulike deler av journalen, og hver del inneholder dokumenter som omhandler samme diagnose eller behandlingsforløp. Jf. Lawrence L. Weed (1968): «Medical records that guide and teach». I: *New England Journal of Medicine,* s. 593–600 og 652–657.

[323] Selv om denne lovendringen kom relativt sent i arbeidet med avhandlingen, er den viktig for flere sider ved problemstillingen. I stedet for en samlet beskrivelse av hva lovendringene gikk ut på, tas de enkelte elementene opp der de får betydning for drøftingen.

[324] « … opplysninger som det kan gis tilgang til i en elektronisk pasientjournal, versus opplysninger som det ikke kan gis tilgang til, må ha en 'grense' mellom seg. I praksis vil denne grensen innebære at de opplysninger som antas å være nødvendige for helsehjelp til pasienten må være avgrenset og strukturert på en bestemt måte.» Ot.prp. nr. 51 (2008-2009), s. 35.

Flertallet i komiteen, som gir sin tilslutning til å bruke helseopplysninger over virksomhetsgrenser, gir også uttrykk for at en forutsetning for denne tilslutningen er regulering og tiltak, herunder strukturering av journalene, som ivaretar prinsippet om at det kun gis tilgang til nødvendige helseopplysninger.

> Flertallet merker seg at det ved bruk av elektroniske systemer alltid må gjøres en vurdering/forhåndsvurdering av om opplysninger i en journal kan deles med annet helsepersonell som kan ha behov for disse, for å kunne tilby pasienten nødvendig helsehjelp. Flertallet er enig i at denne vurderingen må gjøres ved registreringen av opplysningene. Uansett må journalene være strukturert slik at andre som yter helsehjelp, kun gis tilgang til nødvendige helseopplysninger. Flertallet forutsetter at det blir gjort tilpasninger i de elektroniske journalsystemene, slik at de i alle deler av helsevesenet blir strukturert slik at nødvendige helseopplysninger kan skilles fra annen sensitiv personinformasjon.[325]

Sitatet ovenfor viser at det ligger en forventning i lovens motiver om at strukturering av innholdet i journalene i økende grad kan bli gjenstand for direkte regulering eller annen form for normerende standardisering.

5.1.1.3 Opplysninger som er nødvendige for styring, medbestemmelse og etterprøving

Hvilke helseopplysninger dokumentasjonsplikten resulterer i, følger av en relativt åpen rettslig standard, med henvisning til god yrkesskikk, relevans og nødvendighet.[326] Det er altså i liten grad angitt konkret hvilke typer opplysninger om pasientens helse eller om helsehjelpen som må til for å oppfylle plikten.[327] Rett etter den åpne angivelsen av hvordan faglige aktiviteter skal dokumenters følger krav om også å nedtegne eller registrere opplysninger som ikke er direkte knyttet til helsehjelpen, men som er nødvendige for å oppfylle visse andre plikter.[328] Denne siden ved dokumentasjonsplikten har heller ikke særlig detaljert utforming, men den er likevel mindre åpen for skjønn og egne vurderinger fra den som dokumenterer. Emnet for disse opplysningene er behandlingen av helseopplysninger, og ikke pasientens

[325] Innst.O. nr. 110 (2008-2009), s. 3.
[326] «Journalen skal føres i samsvar med god yrkesskikk og skal inneholde relevante og nødvendige opplysninger om pasienten og helsehjelpen, … » helsepersonelloven § 40(1), frem til første komma.
[327] Det påligger imidlertid den databehandlingsansvarlige å ha oversikt over hvilke typer helseopplysninger som behandles, i forbindelse med meldeplikt til Datatilsynet, helseregisterloven § 30(1)(5). Typer helseopplysninger er også i mange tilfeller spesifisert i ulike registerforskrifter.
[328] « … samt de opplysninger som er nødvendige for å oppfylle meldeplikt eller opplysningsplikt fastsatt i lov eller i medhold av lov. Journalen skal være lett å forstå for annet kvalifisert helsepersonell.» (Resten av § 40(1)), og: «Det skal fremgå hvem som har ført opplysningene i journalen» (§ 40(2)).

helse som sådan.[329] Disse opplysningene kan ses som en del av en litt større gruppe opplysninger, som er nødvendige for styring, medbestemmelse og etterprøving ved behandling av helseopplysninger.[330] Krav til å registrere opplysninger for styring, medvirkning og etterprøving er i beskjeden utstrening angitt konkret i lov og forskrift. I noe større grad er slike krav implisitte, som en form for logisk nødvendighet.

De tydeligst konkretiserte kravene til slike opplysninger finner man blant kravene til journalens innhold.[331] Innholdskravene dreier seg dels om å dokumentere hvilken medbestemmelse pasienten har gjort gjeldende, enten det gjelder medbestemmelse om den medisinske behandlingen eller om informasjonsbehandlingen, og dels om å dokumentere faktisk videreformidling av helseopplysninger. Krav til å registrere opplysninger om behandlingen av helseopplysninger er imidlertid ikke noe som bare gjelder for pasientjournaler, det finnes også for en del andre typer registre.[332]

Eksemplene så langt gjelder krav til opplysninger om behandling av helseopplysninger som skal tas inn i journaler og andre helseregistre. Det kan imidlertid være hensiktsmessig også å inkludere opplysninger som genereres automatisk, som biprodukter av informasjonsbehandlingen, men som ikke nødvendigvis tas inn i helseregisteret.[333] Krav til å logge visse aktiviteter, for å kunne etterprøve informasjonsbehandlingen, finnes i beskjedent omfang i

[329] Selv om dette ikke er opplysninger som direkte sier noe om pasientens helse, kan man anta at de ofte vil omfattes av den formuleringen i legaldefinisjonen som fanger opp randsonen, « … og andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold, som kan knyttes til en enkeltperson», helseregisterloven § 2(1)(1).

[330] Det savnes en mer treffende betegnelse for denne typen opplysninger. Den andelen av slike opplysninger som skal eller bør inngå som opplysninger i selve pasientjournalen er i noen sammenhenger plassert under den lite beskrivende betegnelsen «basisopplysninger», jf. Torbjørn Nystadnes (2007b): «EPJ Standard del 2: Tilgangsstyring, redigering, retting og sletting», s. 65.

[331] Pasientjournalforskriften § 8. Dette omfatter blant annet hvem som samtykker for pasient som ikke har samtykkekompetanse (bokstav c), informasjon som er gitt til pasienten, eller hvorvidt pasienten har villet benytte sin rett til ikke å vite (bokstav i), pasientens samtykker til eller reservasjoner mot både helsehjelp og informasjonsbehandling, samt «pasientens øvrige reservasjoner, krav eller forutsetninger» (bokstav j), om det er gjort gjeldende rettigheter som innsyn i journal og krav om retting og sletting, utfallet av dette (bokstav k), utveksling av informasjon med annet helsepersonell (bokstav l), om det er gitt opplysninger til politi, barneverntjenesten, sosialtjenesten mv., og om samtykke er innhentet fra pasienten eller den som har kompetanse til å avgi samtykke i saken (bokstav q).

[332] Et eksempel er «samtykkeadministrative opplysninger for sykdoms- og kvalitetsregistre», i Norsk pasientregisterforskriften, 7. desember 2007 nr. 1389 § 1-6(3)(f). Et mer indirekte krav til å registrere opplysninger om behandlingen av helseopplysninger, i samme forskrift, følger av at «[r]egistrerte har rett til innsyn i utleveringer som gis i personidentifiserbar form.», § 5-1(1)(2). Et eksempel som gjelder et annet register er opplysning om hvorvidt den registrerte har benyttet sin rett til å reservere seg mot utlevering av opplysninger fra egenandelsregisteret, egenandelsregisterforskriften, 18. desember 2009 nr. 1639 § 5(1)(8) jf. § 6.

[333] Den alminnelig brukte betegnelsen på en samling opplysninger som genereres fra informasjonsbehandlingen er *logger*. Forskjellige aktiviteter i et IT-system kan generere en eller flere logger med opplysninger som lagres adskilt fra det systemet som genererer dem. Loggene kan skrives ut og leses manuelt, eller undersøkes med egen spesialisert programvare for formålet. Særlig relevant for denne avhandlingen er ulike typer tilgangslogger.

lover og forskrifter.[334] Mer konkrete angivelse av innholdet i logger finnes det bare små spor av lenger ned i regelhierarkiet.[335]

Som en oppsummering av helt generelle hovedtendenser for helseopplysningers tilblivelse og form, kan man si at de medisinske opplysningene blir til ved at helsepersonell oppfyller en opplysningsplikt, basert på faglig skjønn og god yrkesskikk, i samspill med en hovedsakelig faglig, og i mindre grad rettslig, normering fra et bredt spekter av nasjonale og internasjonale premissgivere. Tilblivelsen av opplysninger om behandlingen av helseopplysninger, som er nødvendige for styring, medbestemmelse og etterprøving, blir til gjennom en noe større grad av rettslig normering.[336]

5.1.2 Opplysningenes kvalitet

Hva kvalitet er, og hvordan det kan oppnås og helst forbedres, er i seg selv et stort emne. I helsesektoren er kvalitet et flerdimensjonalt begrep.[337] Rettslig normering av kvalitetssikring vil ofte ha form av en internkontrollbasert metode, en plikt for virksomheter til å etablere et egnet rammeverk som de selv følger opp, og som også er inspiserbart for eksterne organer.

På det personopplysningsrettslige området har krav til opplysningers kvalitet relativt lang historie, det ble under en viss tvil tatt med som et av de grunnleggende prinsippene i OECDs retningslinje i 1980.[338] Dette kvalitetsbegrepet har to hoveddimensjoner. Den ene er relevans og tilstrekkelighet for formålet, den andre dreier seg om graden av samsvar mellom represen-

[334] Ved endringsloven 19. juni 2009 nr. 68 ble følgende tatt inn som nytt 6. ledd i helseregisterloven § 13: «Den registrerte har rett til innsyn i logg fra behandlingsrettet helseregister om hvem som har hatt tilgang til helseopplysninger om ham eller henne.» Denne bestemmelsen inngikk ikke i departementets forslag til lovendring, den ble tilføyd og begrunnet av stortingskomiteen. Innst.O. nr. 110 (2008-2009), s. 7. Krav til logging finnes også i enkelte av registerforskriftene, for eksempel i Norsk pasientregisterforskriften § 4-2(2) annet punktum: «Det skal også etableres systemer for logging av elektroniske spor ved all tilgang til registeret.»

[335] For eksempel finner man noen bransjeinterne krav til innhold i logger i «Støttedokument – Faktaark nr. 15» av 26. juni 2006, som er underliggende detaljdokumentasjon for sikkerhetsnormen.

[336] Kravene til slike opplysninger utgjør likevel et beskjedent innslag av reguleringen av behandlingen av helseopplysninger. Store deler av de relevante helserettslige og personopplysningsrettslige reglene om behandling av helseopplysninger (som er nærmere drøftet i kapittel 6) er uten betydning for hvilke opplysninger som blir til.

[337] Både nasjonale og internasjonale helsebyråkratiske definisjoner omfatter forskjellige aspekter som at helsetjenesten virker, er sikker, involverer pasientene, utnytter ressurser, er rettferdig etc., jf. Sverre Grepperud (2009): «Kvalitet i helsetjenesten – hva menes egentlig?». I: *Tidsskrift for Den norske legeforening,* s. 1112–1114. Kronikkens konklusjon er at kost/nytte-vurderinger også bør vektlegges, fordi en forbedring langs alle dimensjoner ikke nødvendigvis gir gode samfunnsmessige løsninger når ressursene er knappe.

[338] *The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* (1980), s. 15: Paragraph 8, «Data Quality Principle», lyder «Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.»

tasjon og det som representeres. Varianter av dette kvalitetsbegrepet er nedfelt både i EUs personverndirektiv og i norsk lov.[339]

Forholdet mellom disse to kvalitetsdimensjonene er ikke helt uproblematisk. Et generelt utgangspunkt er at formålsdimensjonen vil være styrende for representasjonsdimensjonen. For eksempel kan en grad av medisinsk uførhet være tilstrekkelig presis som informasjon om hvor godt en pasient kan delta i visse sammenhenger, men ikke tilstrekkelig for å foreslå egnet behandling. Korrekt opplysning – om samme pasient og samme tilstand – kan for det ene formålet være en prosentsats, og for det andre formålet være en diagnosekode kombinert med detaljerte notater i fri tekst. Ut fra dette generelle utgangspunktet vil det være gunstig for pasientens personopplysningsvern at formålsdimensjonen er styrende, det støtter opp under et prinsipp om ikke å behandle flere eller mer belastende opplysninger enn formålet tilsier.

I noen sammenhenger går imidlertid formålets føring lenger enn bare å gi retning til hva som er en tilstrekkelig, og dermed god nok, representasjon. Formålet kan også diktere at en gal representasjon i visse tilfeller skal opprettholdes. Dersom en lege har stilt feil diagnose, og dette flere år senere oppdages og korrigeres, kan legen ha mottatt refusjon på bakgrunn av kodene som ble tilordnet tidligere. Pasientens rett til å få korrigert opplysningene, som han muligens har opplevd som belastende, blir vanskelig å gjøre gjeldende overfor Helseøkonomiforvaltningen som har betalt ut refusjon til legen. Formålet for legens videreformidling av diagnosen til Helseøkonomiforvaltningen var å føre kontroll med refusjonskravet. Som refusjonsgrunnlag kan en gal diagnose, som senere er endret, fremdeles være en opplysning med rett kvalitet uten at det på noe tidspunkt var rett uttrykk for pasientens tilstand.[340] Formålsdimensjonen gir den databehandlingsansvarlige virksomhet, som bestemmer og definerer formålet, vesentlig innflytelse over fastleggingen av kvalitetskriteriene. Terskelen for å få korrigert opplysninger som er relevante for formålet kan være høy, selv om representasjonskvaliteten er tvilsom. En pasients rett til å få korrigert journalen, eller andre helse-

[339] I EP/Rdir 95/46/EF artikkel 6(1), og personopplysningsloven § 11, er begge disse dimensjonene del av de grunnleggende kravene til lovlig behandlingen av personopplysninger, de er også omfattet av handlingsregler som krav til å fastsette formål for behandlingen. Helseregisterloven § 11 omfatter bare formålsdimensjonen, og ikke samsvarsdimensjonen ved opplysningenes kvalitet. Koblingen mellom kvalitet og virksomhetens internkontroll er tydeliggjort i personopplysningsloven § 14 og helseregisterloven §§ 16 og 17.

[340] Som et utgangspunkt skal imidlertid Helseøkonomiforvaltningen slette opplysningene når det ikke lenger er behov for dem for deres egne formål. Lagringstid kan da for eksempel være diktert av regnskapsregler eller arkivregler. Dersom den gale diagnosen i dette tilfellet føles spesielt belastende, kan imidlertid Datatilsynet, som et enkeltvedtak, og etter at Riksarkivaren er hørt, kreve at opplysningene likevel slettes, jf. personopplysningsloven § 27(3). Det er personopplysningsloven og ikke helseregisterloven som får anvendelse i dette eksempelet, jf. folketrygdloven, 28. februar 1997 nr. 19 § 21-11a (5).

opplysninger eller personopplysninger,[341] er dermed i begrenset utstrekning en rettighet som sikrer en representasjonskvalitet som ligger nærmere virkeligheten slik pasienten kjenner den.

Representasjonskvalitetens idégrunnlag er et aristotelisk, korrespondansebasert kriterium for hva som er gode nok opplysninger.[342] Forutsetningsvis er opplysningene riktige hvis det er godt samsvar mellom opplysning og virkelighet. En mer elaborert inndeling av korrespondansekriterier for datakvalitet er å dele det opp i tre typer egenskaper, presisjon, kompletthet og korrekthet.[343] Presisjon referer til detaljnivået i dataenes beskrivelse av noe i verden. Kompletthet dreier seg om hvorvidt dataene er nødvendige og tilstrekkelige som beskrivelse. Presisjon og kompletthet kan sies å henge sammen med intensjonen bak en representasjon, hvor nøyaktig man har tilsiktet at dataene skal beskrive noe i verden. Disse egenskapene har betydning for om en representasjon er *velvalgt*. Korrekthet er et mål for hvor god korrespondanse det faktisk er, om dataenes beskrivelse er «sann», innenfor den tilsiktede graden av nøyaktighet. Korrekte data har betydning for om en representasjon er *vellykket*.

En del av kvalitetssikringsarbeidet for helseregistre dreier seg om konkrete fremgangsmåter for å avdekke feilregistreringer. Et eksempel på noen slike fremgangsmåter er beskrevet i et rundskriv fra Helse- og omsorgsdepartementet, som skiller mellom tekniske kontroller for å avdekke opplagte feil, «for eksempel … dersom menn føder barn eller kvinner får prostatakreft,» kontroll ved å koble opplysninger med andre registre som skal inneholde deler av de samme opplysningene, eller den kvalitetssikring man får ved at registrene i praksis brukes til forskning.[344] En utredning om pseudonyme helseregistre fra 1993 vier omfattende drøftinger til opplysningenes kvalitet, og kvalitetssikringsarbeid. Blant annet gir den en relativt nyansert klassifisering, i form av en systematikk som skiller mellom tilfeldige og systematiske feil.[345] En av de systematiske feilene som beskrives, under betegnelsen informasjonsskjevhet, er eksemplifisert med at gradvise endringer over tid i en diagnoses meningsinnhold, kan føre til endringer i hvor ofte samme sykdom blir meldt, selv om reglene for hva som skal registreres er stabile. Opplysningenes felles referanseramme, og omstendighetene rundt opplysningenes tilblivelse, er flyktige. Derfor er aktualitet et sentralt element ved representasjonskvaliteten.

---

[341] Etter henholdsvis pasientrettighetsloven § 5-2, helseregisterloven § 26(1) og personopplysningsloven § 27(1).
[342] Parafrasert til «å si om det som er at det er, eller om det som ikke er at det ikke er» som kriterium for sannhet, jf. Donald Davidson (1996): «The Folly of Trying to Define Truth». I: *The Journal of Philosophy,* s. 263–278. (s. 265).
[343] Denne tredelingen av korrespondanseegenskaper er fra Lee A. Bygrave (1996): *Ensuring right information on the right person(s): legal controls of the quality of personal information, Part 1*.
[344] Jf. avsnittet «nærmere om kvalitetssikring av opplysningene i registeret» i *Pseudonyme helseregistre, rundskriv fra Helse- og omsorgsdepartementet.* (2005), s. 13.
[345] NOU 1993:22, kapittel 8.2.6. Denne utredningen kan betraktes som en del av forarbeidene til helseregisterloven, til tross for at den ble avgitt før personverndirektivet ble vedtatt.

Et spørsmål, som har kommet opp i ulike sammenhenger, er om pasientens innsynsrett vil føre en til endringer i måten helsepersonell dokumenterer på.[346] En eventuell slik forskyvning betyr ikke nødvendigvis at det som skrives er mindre korrekt, men det indikerer likevel at kvaliteten kan være avhengig av flere faktorer enn hvor riktig den faglige vurderingen er og hvor hensiktsmessig den valgte fremstillingsformen er. Uten å kunne si at belegget er veldig overbevisende, synes det foreløpig som om pasienters innsynsrett har hatt relativt liten effekt på hvordan helsepersonell dokumenterer. En amerikansk metaanalyse, som har gjennomgått en del forskjellige studier av ulike effekter av pasienters innsynsrett, fant visse virkninger for lege-pasientrelasjonen, men ingen særlige effekter på hva som ble skrevet i journalene.[347] Det resultatet er også i samsvar med følgende betraktning i en lingvistisk studie av psykiatriske journaler:

> Både jeg og psykiatriske fagfolk hadde nok umiddelbare forventninger om at den judisielle bestemmelsen om pasienters innsynsrett ville føre til forskyvninger i journalskriften. Til min forbauselse har jeg ikke kunnet konstatere noen vesentlig forandring. … Journalskriften har alltid vært tilbakeholdende og tildekkende. Det ikke å fornærme pasienten ved lesning i ettertid er bare ett av mange hensyn å ta.[348]

De ovenstående eksemplene dreier seg om kvalitetsproblemer som den som dokumenterer normalt ikke er seg bevisst. Andre problemer ved representasjonskvaliteten, som det også kan være praktisk vanskelig å avdekke og gjøre noe med, er ulike grader av bevisst desinformasjon eller feilføring. For det første kan pasienten selv overdrive symptomer for å oppnå resept på sitt favorittpreparat, eller underslå symptomer for å slippe formaninger om å endre livsstil. Dokumentasjonen som nedtegnes kan være samvittighetsfull og reflektere helsehjelpen, men uten at det stemmer med pasientens tilstand. For det andre vil strategisk feilføring eller feilkoding fra helsepersonellets eller virksomhetens side kunne føre til et misforhold mellom opplysningene og pasientens tilstand. Tilsiktede feilføringer kan for eksempel skyldes et ønske om å dekke over en uforsvarlig handling, eller å oppnå mer gunstig økonomisk dekning for den helsehjelpen som ytes.[349]

---

[346] I sykejournaldommen, Rt. 1977 s. 1035, siterer førstvoterende noen utdrag fra en skriftlig rapport fra en av de sakkyndige (professor i samfunnsmedisin, Axel Strøm), som inneholder flere argumenter for og mot å la pasienter få innsyn. Et av motargumentene lød «Hvis det blir åpnet en alminnelig adgang for pasientene til å lese sin journal, vil det måtte føre til en omlegging av journalføringen. En slik omlegging vil gjøre journalen mindre egnet som arbeidsdokument for avdelingen og gjøre journalskrivingen mer tidkrevende. En form for dobbelt bokføring vil med overveiende sannsynlighet tvinge seg frem.» (på s. 1045–1046).

[347] Stephen E. Ross og Chen-Tan Lin (2003): «The effects of promoting patient access to medical records: a review». I: *Journal of the American Medical Informatics Association,* s. 129–138. (s. 135).

[348] Aaslestad (2007), s. 193.

[349] Dette var mulige forklaringer på en del feilkoding i innrapporterte data i en empirisk undersøkelse, Linda Midttun m. fl. (2003): «Er det sammenfall mellom journalopplysninger og innrapporterte data? En studie av 500

Feil koding av opplysninger kan også være en bevisst, men uskyldig ment handling for å komme rundt en stivbent formalisme i informasjonssystemet. Et illustrerende eksempel er en situasjon fra desember 2005, der apotekene etter regelverket skulle utlevere en billigere variant av en medisin mot beinskjørhet enn den legen hadde anført, dersom ikke legen hadde krysset av for reservasjon mot at det leveres ut annet preparat med samme virkestoff. Den billigere medisinen som skulle brukes var imidlertid ikke tilgjengelig fra apotekene på det tidspunkt den skulle ha vært det, dermed krysset apotekene selv av for legereservasjon i datasystemet. Avkrysningen var «nødvendig» for at apoteket skulle få levert ut den dyrere medisinen uten problemer. Apotekene skal ha blitt oppfordret til å håndtere problemet på denne måten av Norsk Apotekerforening, etter avklaring med Statens legemiddelverk. Legeforeningen anså på sin side dette som dokumentfalsk, og pekte på at praksisen kunne føre til senere problemer for legen, dersom en kontroll viser at avkrysningen ikke gjenspeiler en begrunnet vurdering i pasientjournalen.[350] De som anbefalte denne pragmatiske omgåelsen av et formalistisk hinder tenkte neppe over at det kunne ha utilsiktede konsekvenser i ettertid.

Opplysninger som ikke er korrekt kodet har vært gjenstand for en del oppmerksomhet, blant annet har Riksrevisjonen undersøkt kvaliteten på kodingsarbeidet i flere sykehus. Riksrevisjonen gjennomgikk primært helseforetakenes systematiske arbeid for å sikre kvaliteten i kodingsarbeidet, altså en form for systemrevisjon. Konklusjonene gjaldt først og fremst svakheter i dette arbeidet. Som del av kontrollen ble det også gjennomført en spørreskjemaundersøkelse blant leger. De årsakene som figurerte øverst i legenes vurdering var at kodeverket som sådan var vanskelig, og at de fikk for lite opplæring.[351]

At ferdighetene hos den som dokumenterer kan ha en del å si for representasjonskvaliteten er ikke noe som bare gjelder det å knytte sine vurderinger og beslutninger til rett kode i et stort kodeverk. I en gjennomgang av psykiatriske journaler over et langt tidsrom reflekterer forfatteren ved et par anledninger over verktøyenes virkning på det som skrives i fri tekst. Paradokset er at gode verktøy kan se ut til å redusere journalnotatenes kvaliteter som tekst.[352]

---

pasientopphold ved norske somatiske sykehus i 2001». Helt siden utgiftsrefusjoner basert på diagnoserelaterte grupper (DRG) var på forsøksstadiet i USA, på 1970- og begynnelsen av 80-tallet, har det vært en del oppmerksomhet om ulike varianter av strategisk koding, fra det nær legitime til noe som ligner mer på svindel. Jf. Donald W. Simborg (1981): «DRG creep: a new hospital-acquired disease». I: *New England Journal of Medicine,* s. 1602–1604.

[350] Situasjonsbeskrivelsen er basert en ensidig kilde, men kan likevel egne seg som illustrasjon på «uskyldig ment» strategisk koding. *Urettmessig påføring av legereservasjon i apotek.* (2005).

[351] *Riksrevisjonens undersøkelse av kodekvaliteten ved helseforetakene.* (2006), s. 7 og s. 26.

[352] «Parallelt med at journalens ytre form stadig blir mer velordnet gjennom raffinert layout; fra håndskrift til skrivemaskin til dagens avanserte tekstbehandlingsprogrammer, så taper helsepersonellet sine tidligere ferdigheter som skrivende mennesker.» Aaslestad (2007), s. 29.

Verktøyenes virkning er et moment som leder over til et annet aspekt ved representasjonskvaliteten. Informasjonssystemenes kvalitet er en faktor som skiller seg en del fra det som er nevnt ovenfor, men som likevel kan påvirke samsvaret mellom opplysning og virkelighet.[353] Det omfatter både teknisk kvalitet, holdbarheten av de tolkninger som er gjort under systemutvikling, forståelighet, robusthet og hvor vedlikeholdsvennlig systemet er.

De mange og sammensatte faktorene som påvirker opplysningenes kvalitet antyder at problemene knyttet til kvalitet er iboende i opplysningenes tilblivelse og form. Riktig tasting og god opplæring er viktig, men langt fra hele bildet. Det blir for enkelt å betrakte god kvalitet som noe man får hvis man er flink, nøyaktig og samvittighetsfull, mens uflaks, lemfeldighet og ukyndighet gir dårlig kvalitet. Forbedret kvalitet kan også oppnås gjennom bedre organisatoriske prosesser, bedre systemdesign, og kloke tilpasninger til endringer i omgivelsene i et tempo som tilstrekkelig mange vil kunne tilpasse seg. Dårlig kvalitet kan, ved siden av slett arbeid med å designe eller bruke systemer, skyldes at utydelige eller grenseløse formål for informasjonsbehandlingen fører til for lite kunnskap om hvilken representasjonskvalitet som er nødvendig for det enkelte formål. En helseopplysning kan være en velegnet representasjon av en del av virkeligheten, til et angitt formål. Det er imidlertid en annen og ny vurdering som må til for å bestemme om samme opplysning også er egnet til å bli videreformidlet og brukt av andre personer og i en ny sammenheng.

5.1.3 Helseinformasjon som ikke er personopplysninger

Legaldefinisjonen av personopplysninger er «opplysninger og vurderinger som kan knyttes til en enkeltperson.»[354] På tilsvarende måte er det å kunne knyttes til enkeltperson en av de definerende egenskapene for helseopplysninger. De særskilte behovene for å beskytte opplysningene henger sammen med nettopp denne egenskapen. For mange samfunnsnyttige formål vil imidlertid opplysninger eller informasjon om helse kunne formidles godt nok uten å knyttes til enkeltpersoner. Når først opplysningene kan knyttes til en enkeltperson, kan det i utgangspunktet være svært bredt hva som egentlig omfattes av personopplysningsbegrepet. Innen personvernteori anses det ofte som mest hensiktsmessig å legge til grunn et vidt personopplysningsbegrep, mens regelverket anvendes fleksibelt, tilpasset personvernrisikoen.[355]

[353] Bygrave (1996).
[354] Personopplysningsloven § 2(1)(1).
[355] Thomas Olsen (2009): «Personvernøkende identitetsforvaltning», s. 104–107, legger til grunn en slik forståelse av personopplysningsbegrepet, særlig med bakgrunn i personverndirektivets definisjon og uttalelser fra Artikkel 29-gruppen.

Dersom man lykkes i å formidle informasjonen på en slik måte at det er tilstrekkelig sikkert at den *ikke* kan knyttes til en enkeltperson, faller behovene for å regulere og kontrollere tilgang og videreformidling bort. Slik informasjonen havner utenfor avhandlingens emne. Det følgende beskriver og eksemplifiserer noen typer informasjon som kan falle utenfor.

5.1.3.1 Generell informasjon og generaliserte kasuistikker

Generell helseinformasjon kan betraktes som informasjon som ikke er basert på opplysninger om identifiserbare enkeltpasienter i utgangspunktet. Et eksempel kan være inndelingen i risikogrupper på informasjonsnettstedet om «svineinfluensaen».[356] Selv om arbeidet med å definere risikogrupper på et tidspunkt har dreid seg om å analysere enkelttilfeller, er det likevel ingen personopplysninger involvert i de egenskapene som karakteriserer en risikogruppe.

En variant av generell informasjon der det er nødvendig å være litt mer omhyggelig, er generaliserte kasuistikker. Det som presenteres er gjerne en *persona*, en ikke-eksisterende person, representert ved et tilfeldig fornavn eller forbokstav. Helseinformasjonen som knyttes til denne personaen skal være realistiske, men bør ikke ha en bestemt enkeltperson som opphav. Tilstander, samtaler, behandling med videre som knyttes til personaen kan bygge på trekk fra og erfaringer med flere forskjellige personer. Personaen er derfor ikke identisk med en enkeltperson. Dette er ofte brukt som en pedagogisk formidlingsform blant helsepersonell som skriver for en bred målgruppe.[357] I praksis kan det være vanskelig å etterprøve om en forfatter har lykkes godt nok i å abstrahere personaen tilstrekkelig til at enkeltpersoner ikke kan identifiseres. Det får man ikke svar på før en reell pasient eventuelt er gjenkjent. Et utvalg personaer kan også være generaliseringer som brukes til klassifiseringsformål, de er en metodisk slektning av idealtyper.

5.1.3.2 Fjerning av personidentifiserende kjennetegn

Anonyme opplysninger er definert som «opplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til enkeltperson.»[358] Definisjonen angir at det dreier seg om fraknytting fra enkeltpersonen, men uten å angi kriterier for hvor god anonymiseringen behøver være.[359]

---

[356] Helsedirektoratet, «Pandemi – Myndighetenes nettside om pandemisk influensa»: *http://www.pandemi.no/*.
[357] For eksempel har Gro Nylander og Finn Skårderud brukt denne formen en del i popularisert faglitteratur.
[358] Helseregisterloven § 2(1)(3).
[359] Det ligger imidlertid et implisitt krav til anonymiseringens effektivitet i kontrasten til to andre definisjoner i samme paragraf i helseregisterloven, begrepene avidentifiserte og pseudonyme helseopplysninger, som begge faller innenfor kriteriet «kan knyttes til enkeltperson».

Flere av helseregisterforskriftene angir en nokså vid ramme for hvilken bruk av registeret som er tillatt så lenge resultatene fremkommer i anonymisert form. Et eksempel er forskriften til Norsk pasientregister.[360] I Helse- og omsorgsdepartementets kommentar til hvordan forskriftsbestemmelsen skal forstås, publisert sammen med forskriften i Norsk Lovtidend, skriver de:

> Hvorvidt statistikken eller tabelldataene er tilstrekkelig anonymisert, må vurderes i det enkelte tilfelle. Ved publisering av tabeller på lokalt og regionalt nivå har det i praksis vært lagt til grunn 4 eller 5 enheter. Det innebærer at en ikke oppgir enheter som svarer til færre enn 4 eller 5 personer.[361]

Denne operasjonaliseringen er noe mer restriktiv enn bare å fjerne personentydige kjennetegn. Ut fra denne tommelfingerregelen vil det av og til være nødvendig å velge mindre nyanserte måter å gruppere informasjon på, for å sikre at et informasjonselement aldri representerer et for lavt antall enkeltpersoner.

En generalisert variant av denne tommelfingerregelen, som det er henvist til i en del litteratur om personvernøkende teknologier, er formalisert under betegnelsen k-anonymitet.[362] En datamengde er «k-anonym» dersom det aldri er færre enn k personer som deler de kombinasjonene av egenskaper som finnes i datamengden.[363] For å oppnå k-anonymitet kan man enten generalisere, for eksempel ved å slå sammen flere verdier av en opplysningstype til et videre intervall av verdier, eller undertrykke, altså utelate, opplysningstyper som gjelder færre enn k personer. Samme kildematerialet kan gi opphav til flere ulike k-anonyme datamengder, teorier om k-anonymitet drøfter blant annet strategier for å finne de datamengdene som bevarer størst mulig andel av kildematerialets opplysninger etter anonymiseringen.

Legaldefinisjonen av anonyme opplysninger omfatter ikke bare anonymisert statistikkproduksjon. Det kan også dreie seg om å beskrive et enkelttilfelle, som i utgangspunktet er basert på en reell person, på en slik måte at vedkommende ikke kan identifiseres. Den som skriver vurderer konkret hva som må utelates for å unngå identifiserbarhet. Resultatet vil ligne en del på en fiktiv persona, som beskrevet ovenfor, men fallhøyden er større fordi det finnes en faktisk enkeltperson bak de opplysningene som fjernes.[364] Ettersom det er vanskelig å gi

[360] Norsk pasientregisterforskriften § 3-1.
[361] Norsk Lovtidend avd. I, 2007, hefte 12 s. 1720.
[362] Pierangela Samarati og Latanya Sweeney (1998): «Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression».
[363] Praksisen som det vises til i kommentaren til forskriften kan altså beskrives som 'k-anonymitet, der k=4 eller k=5'.
[364] En situasjon der spørsmålet om anonymisering kom på spissen, oppsto med et brev fra fire barnevernsansatte til bystyret i Oslo. De eksemplifiserte innvendinger mot organisatoriske endringer ved å vise til sin beskrivelse av tolv anonymiserte barn. I utgangspunktet var de anonymisert til kjønn og alder, men det var også en omtale av

generelle svar på hva som vil være tilstrekkelig anonymisering, bør det forventes at den som formidler anonymiserte opplysninger utviser stor forsiktighet.

Noe som kan ligne anonymisering, og som pasienter i mange tilfeller selv vil kunne oppfatte slik, er sosiale pasientnettverk på Internett, der hver pasient selv kan velge i hvor stor grad de ønsker å tilkjennegi sin egentlige identitet.[365] Pasientene deler erfaringer og synspunkter med andre pasienter, ofte med utgangspunkt i en felles diagnose.[366] I denne typen kanaler er det ikke egentlig dekkende å betrakte det valget pasienten treffer om å skjule sin identitet som reell anonymitet. Koblingen mellom identitet og representasjon forvaltes av en operatør som vet mer om hvem pasienten er enn det pasienten selv har valgt å synliggjøre på nettet. Den valgte graden av kamuflering vil gi pasienten en opplevelse av å kunne være skjult for andre personer i nettverket, men konfidensialiteten er sårbar både for tekniske feil, egen manglende forståelse av hvordan ulike «anonymiseringsvalg» fungerer, og at andre brukere kan gjenkjenne pasienten gjennom ulike detaljer i de erfaringene man velger å dele. Uavhengig av hvor god eller pålitelig muligheten for å skjule egen identitet er, vil rene sosiale pasientnettverk befinne seg utenfor den formelle reguleringen av tilgang og videreformidling så lenge pasientnettverket ikke står i kontakt med helsepersonell.

5.1.3.3 Helseopplysninger i skjønnlitteraturen

Helseopplysninger, som tema for regulering og kontroll, er opplysninger om virkeligheten, og i virkeligheten. I skjønnlitteraturen er det nærliggende å låne inn ett og annet element fra virkeligheten, som omformes til litteratur. Helter og skurker med hvit frakk og stetoskop har aldri vært mangelvare i skjønnlitteraturen, og romanfigurers sykelighet er det heller ikke noe å si på. Avgrensningsspørsmålet her blir omtrent det samme som for formidling ved å skrive om en abstrahert persona. Det faller helt utenfor feltet, også utenfor definisjonen av anonyme opplysninger, ettersom utgangspunktet forutsetningsvis er en fiksjon. Det er først og fremst forfatterens etiske plikt å unngå at helseopplysninger avdekkes til skade for hans eventuelt gjenkjennbare modell.

Det kan imidlertid – mest som kuriosa – være verdt å nevne noen litt interessante nyere innslag i norske romaner. Enkelte forfattere har oppdaget hvor godt regler og rutiner for behandling av helseopplysninger egner seg som dramatisk stoff. Skjønnlitteraturen får frem et

---

hva slags typer problemer enkelte av barna hadde å stri med, med påfølgende diskusjon om hvorvidt anonymiseringen var tilstrekkelig. *Akutt- og utredningstilbudet for ungdom på åpne institusjoner i Oslo.* (2009).

[365] Sosiale, internettbaserte nettverk på helseområdet omtales av og til som «helse 2.0» eller «pasient 2.0», med en allusjon til det sjargongpregede uttrykket «web 2.0». På engelsk brukes også betegnelsen «Medicine 2.0».

[366] Et kjent, åpent internasjonalt eksempel er nettstedet www.patientslikeme.com.

element som gjerne forsvinner litt i akademisk og teknokratisk litteratur om emnet: Det kan ligge store muligheter for å utøve makt og kontroll, avdekking og tildekking, i de måtene man behandler helseopplysninger på. Tre små eksempler gjengis, mest for fornøyelsens skyld.

Det første utdraget dreier seg om meldeplikter og kryssende kollegiale hensyn. I romanen *Unaturlig dødsfall meldes*[367] dør en pasient. Dødsfallet har sammenheng med uforsvarlige handlinger fra en overordnet kirurg. En yngre kollega manipuleres til å signere en ufullstendig dødsattest, og får i ettertid en tilrettevisning fra fylkeslegen.[368] Romanen problematiserer faren for maktmisbruk i spenningsfeltet mellom formell meldeplikt, uskrevne regler, rang og kollegiale hensyn.

> [D]et er hun … som har synet liket og konstatert at døden er inntrådt, som fyller ut dødsattesten, som også har ansvaret for dette: om det skal meldes som et unaturlig dødsfall, eller ikke. I så fall må hun nærmest angi en kollega. Slik vil det bli oppfattet innenfor veggene, og kanskje utenfor også, en mistanke om skyld. De åpne bøkers politikk er en doktrine offentlige helsemyndigheter prediker. I det virkelige livet skal man ha en godt begrunnet mistanke. Og bred rygg.

I romanen *Legen som visste for mye*[369] er legens pasientarkiv både et uttrykk for makt, og et verktøy for å utøve makt. Hovedpersonen Mads Helmer er ny lege på Hitra. Flere ganger stusser han over den nylig avdøde Gammeldoktorens pasientbehandling. Dokumentasjonen i det elektroniske journalsystemet er mangelfull og upålitelig. Etter hvert vekkes mistanken om at Gammeldoktoren må ha hatt et uoffisielt arkiv på siden av journalsystemet. Da han omsider får adgang til Gammeldoktorens bolig, viser det seg at arkivet har vært utsatt for et innbrudd. Fra kapittel 23, s. 208:

> Mads kikket på mappene som lå strødd utover gulvet. Hver og en hadde et pasientnavn og en fødselsdato skrevet inn på forsiden. Håndskriften var lett å gjenkjenne. Så hadde han altså hatt rett. Gammeldoktoren hadde virkelig sittet på et eget pasientarkiv, men av helt andre dimensjoner enn han hadde forestilt seg. Han la merke til at det lå linjerte, håndskrevne ark innimellom papirene på gulvet. Det måtte ha vært Gammeldoktorens journalnotater – lagt i pasientmappene etter endt arbeidsdag. Det var derfor han hadde kunnet tillate seg å være så knapp når det gjaldt den elektroniske journalen. Han hadde all informasjon samlet her. I sin egen kjeller.

Betraktningene om dette uoffisielle arkivet fortsetter på s. 210:

---

[367] Marianne Mjaaland (2003): *Unaturlig dødsfall meldes*, sitert fra s. 15.
[368] Skriftlig tilrettevisning var tidligere den mildeste av reaksjonsformene for overtredelse av legeloven eller handlinger i strid med god legeskikk. Skriftlig advarsel var et lite hakk mer alvorlig, og innebar en rett til å forklare seg på forhånd (legeloven [1980], 13. juni 1980 nr. 42, (Opphevet) § 52).
[369] Christer Mjåset (2008): *Legen som visste for mye*, kapittel 23, sitert fra s. 208 og s. 210.

> Dette var ikke bare et pasientarkiv. Det var et etterretningsarkiv. Han kom til å tenke på samtalene han hadde hatt med både Anwar og Zakarias Dahl. Begge hadde nevnt at Gammeldoktoren hadde hatt en finger med i det meste som skjedde her ute på øya. Det var ikke så vanskelig å forstå at han hadde kunnet utøve makt når han satt på sensitiv informasjon om så å si alle døde og levende hitterværinger de siste tretti–førti årene. Mads lot blikket løpe over gulvet og alle papirene som lå og fløt. Noen hadde tydeligvis visst om dette arkivet.

Også sett med pasientens blikk kan journalene være et uttrykk for fagets og institusjonens makt. Romanen *Norske helter*[370] beskriver med bred penn hvordan institusjonen snor seg, og forsøker å beskytte seg, både mot samfunnet utenfor og mot pasientene. Her er det en pasient som er hovedperson, og han har kommet til at snoking i journalene er nødvendig for å finne ut hva som egentlig forgår ved institusjonen.

> Journalene var det nærmeste brukerne kom en biografi; hele livet deres lå der mellom permene: alt som hadde skjedd dem, alle spor etter sykdommer og uregelmessigheter, alle informasjoner om kropp, vekt, fødsel – og død. Sto man med en brukers journal i hånda sto man med et menneske, sa Hølcke, tykkere enn noen roman, mer motsetningsfylt og springende, og fylt til randen av skjebne. Journalen er hellig!
>
> Og det sto virkelig en aura rundt disse journalene. Man senket stemmen litt, når man snakket om dem. Menneskene var så vanskelige å gripe i all sin flyktighet, tenkte jeg, men journalen var konkret, med journalen kunne man snakke.

5.2 IT-systemer der helseopplysninger behandles

Reguleringen av ulike virksomheters opplegg for behandling av helseopplysninger bruker hovedsakelig teknologinøytrale begreper som helseregistre, journaler eller informasjonssystem. Disse begrepene favner videre enn IT-systemer, og fanger også opp de betydelige mengdene dokumentasjon som finnes på papir og andre ikke-elektroniske medier. En virksomhets plikt til å følge opp behandlingen av helseopplysninger er prinsipielt uavhengig av om opplysningene lagres eller formidles elektronisk eller på andre måter. Reguleringens teknologinøytralitet er imidlertid ikke statisk, den kan se ut til å være under noe press. Et mål om ikke å binde reguleringen fast til teknologivalg kan være basert på et ønske om at teknologivalget skal være et mest mulig selvstendig og frivillig valg under den enkelte

[370] Vetle Lid Larssen (2007): *Norske helter*, kapittel 9, sitert fra s. 223.

virksomhets handlingsrom.[371] Et annet mål bak teknologinøytraliteten, som nærmest kan peke i motsatt retning av frivillighetsargumentet, er et ønske om å unngå at reguleringen blir hengende etter den teknologiske utviklingen, og å unngå at reguleringen står i veien for en teknologisk utvikling. Selv om reguleringen på mange områder beholder en teknologinøytral form, legges det likevel opp premisser og føringer som stiller krav til teknologibruk i virksomhetene.[372]

Behandling av helseopplysninger i elektronisk form gjør det både mulig og nødvendig å innlemme regulering og kontroll i IT-systemene. Uttrykket «å innlemme» skal forstås litt løselig, i den forstand at innlemmingen ikke nødvendigvis betyr at kontrollmekanismene må plasseres i samme IT-system. Man gjerne kan basere store deler av dette på egne, separate sikkerhetsmoduler som samvirker med de IT-systemene som inneholder helseopplysningene.

I dette kapitlet presenteres en overordnet klassifisering av IT-systemer der helseopplysninger behandles, hovedsakelig basert på terminologi som brukes i helseinformatisk litteratur. Klassifiseringen er ikke spesielt nyansert, og ikke så detaljert at den omfatter bestemte produktnavn. Hovedgruppene i klassifiseringen følger helseregisterlovens grunnleggende skille mellom behandlingsrettede og ikke-behandlingsrettede helseregistre.[373] Inndelingen i behandlingsrettet og ikke-behandlingsrettet er et uttrykk for et gjennomgående prinsipp om at berettigelsen for behandling av helseopplysninger er forankret i formålet med behandlingen.

Helseregisterlovens registerbegrep omtales i forarbeider og teori som et «logisk registerbegrep».[374] I proposisjonen til helseregisterloven ble dette tydeliggjort:

> Registerbegrepet er her et logisk begrep. Det er ikke en datateknisk definisjon. Et register kan bestå av flere datafiler, og kan fysisk føres flere forskjellige steder. Om-

[371] Frivilligheten er signalisert ved en «kan»-modalitet, blant annet i *helsepersonelloven* § 46(1): «Pasientjournal kan føres elektronisk.» Enkelte nyere bestemmelser i helseregisterloven, §§ 6a og 6b, gjeldende fra juni 2009, bestemmer derimot at de helseregistrene som det der gis hjemmel for *skal* være elektroniske.

[372] Teknologisk standardisering og felles infrastruktur er virkemidler som brukes, og graden av frivillighet i standardiseringen synes å være dalende. Det kommer blant annet til uttrykk i Stortingsmelding nr. 47 (2008-2009), s. 135–136, gjennom en erklæring om at det i større grad skal tas i bruk «tidsfrister» som virkemiddel for standardiseringen. Et konkret eksempel er ikraftsettingstidspunkt for forskrift om elektronisk kommunikasjon (HELFO), som pålegger leger å sende inn refusjonskravene elektronisk, i den forstand at det har blitt en betingelse for refusjon. Samme type elektronisk innsending har tidligere vært et frivillig tilbud, med beskjedne incitamenter.

[373] Behandlingsrettet helseregister er legaldefinert, som «journal- og informasjonssystem eller annet helseregister som har til formål å gi grunnlag for handlinger som har forebyggende, diagnostisk, behandlende, helsebevarende eller rehabiliterende mål i forhold til den enkelte pasient og som utføres av helsepersonell, samt administrasjon av slike handlinger,» helseregisterloven § 2(1)(7). Loven definerer ikke, i bokstavelig forstand, hva som er «ikke-behandlingsrettet». Den betegnelsen brukes her om det som hører inn under definisjonen av helseregistre, *minus* det som hører inn under behandlingsrettede helseregistre.

[374] En sondring mellom fysiske og logiske registre oppsto som en problematisering av hva et register skulle innebære etter den tidligere personregisterloven, 9. juni 1978 nr. 48, (Opphevet). Praksisen som ble etablert pekte etter hvert i retning av logiske registre. Eirik Djønne m. fl. (1987): *Personregisterloven med kommentarer*, s. 29.

> vendt vil en samling opplysninger som er lagret på samme server, ikke nødvendigvis utgjøre et register. Det avgjørende er om det er en logisk sammenheng i registreringen, og at det er den samme myndighet som har ansvaret for registreringen.[375]

Det logiske registerbegrepet innebærer også at det ikke er noen klar sammenheng mellom en «type register» og en «type IT-system». Samme logiske register kan bre seg ut over flere av de typene IT-systemer som er beskrevet i denne overordnede klassifiseringen. Et logisk registerbegrep skiller seg dermed ikke vesentlig fra den innretningen man har i den generelle personopplysningsloven, der reguleringen primært er knyttet til det å behandle personopplysninger, mens registerbegrepet bare har underordnet betydning. Formålsinndelingen, som i helseregisterloven setter et hovedskille mellom behandlingsrettet og ikke behandlingsrettet, har derimot relativt stor betydning for regulering av og kontroll med informasjonsbehandlingen.

5.2.1 Behandlingsrettede helseregistre, hovedsakelig innen en virksomhet

At et helseregister er behandlingsrettet, knytter det til helsepersonellets plikt til å nedtegne eller registrere helsehjelpen i en journal for den enkelte pasient.[376] Legaldefinisjonen av behandlingsrettet helseregister er imidlertid noe videre enn bare å omfatte samlingen av de journalopplysninger helsepersonell har ført.[377] Helsepersonells plikt til å dokumentere i journalen innebærer ikke noe forbud mot at de også fører noen av de samme opplysningene om igjen, og i tillegg eventuelle andre opplysninger utover dokumentasjonsplikten, i andre behandlingsrettede helseregistre enn journalen. Både opplysninger som føres av personer som ikke er autorisert helsepersonell, og opplysninger som ikke nødvendigvis er omfattet av dokumentasjonsplikten, kan høre inn under den klassen av formål som legaldefinisjonen betegner som behandlingsrettede.

Helseregisterloven knytter flere steder bestemmelser som gjelder behandlingsrettede registre til helsepersonellovens bestemmelser om behandling av helseopplysninger. Et eksempel er at betingelsen for å sammenstille opplysninger fra to forskjellige behandlingsrettede registre er at det må være anledning til utlevering etter helsepersonelloven §§ 25, 26 og 45.[378] Denne adgangen til sammenstilling åpner i utgangspunktet en vid adgang til å integrere ulike IT-systemer som brukes i pasientbehandlingen innenfor en virksomhet, så lenge rammene for

[375] Ot.prp. nr. 5 (1999-2000), s. 64
[376] Helsepersonelloven § 39 jf. § 40.
[377] Helseregisterloven § 2(1)(7).
[378] Helseregisterloven § 12(1).

autorisert tilgang til opplysningene overholdes.[379] Det kan også gis tilgang, eller videreformidles opplysninger, mellom behandlingsrettede helseregistre i forskjellige virksomheter.[380] Helseregisterloven snevrer imidlertid inn utvalget av gangbare måter dette kan gjøres på, slik at adgangen til sammenstilling av opplysninger mellom behandlingsrettede helseregistre fremdeles ikke er like vid på tvers av virksomheter som den er innenfor en virksomhet.[381]

Andre eksempler på at helseregisterloven knytter behandlingsrettede registre til helsepersonellovens bestemmelser om behandling av helseopplysninger er reglene om den registrertes rett til innsyn,[382] og plikten den databehandlingsansvarlige har til å rette, slette eller supplere gale eller mangelfulle opplysninger, enten av eget tiltak eller på den registrertes begjæring.[383]

5.2.1.1 Elektronisk pasientjournal (EPJ)

Den bredeste og mest omfattende dokumentasjonen av helseopplysninger om en pasient finnes i pasientjournalen. Journalen står også i en spesiell stilling som rettslig dokumentasjon, både på grunn av dokumentasjonsplikten og fordi innholdskravene omfatter mer enn bare egentlige helseopplysninger. De omfatter i tillegg opplysninger som er nødvendige for å ivareta rettigheter, medbestemmelse og etterprøving. Pasientjournaler er ikke nødvendigvis elektroniske, men det har etter hvert blir svært utbredt. Innføring av EPJ var fullført i nær 80 prosent av helseforetakene i 2008, og påbegynt i en eller annen grad i alle de øvrige. For allmennleger har utbredelsen vært relativt stabil rundt 98 prosent i noen år.[384] Helsepersonelloven stiller ikke krav til teknologi, der heter det at pasientjournalen kan føres elektronisk. I så fall, for elektroniske pasientjournaler, kan det i forskrift gis nærmere bestemmelser, « …

---

[379] Helsepersonelloven § 25 begrenser ikke typene opplysninger, men avgrenser til samarbeidende helsepersonell. Med formuleringen «vedkommende virksomhets pasientadministrasjon», avgrenser § 26(2) i mindre grad personkretsen, men der settes det til gjengjeld klarerere grenser for hvilke typer opplysninger som kan omfattes.

[380] Helsepersonelloven § 45 gir prinsipielt vid adgang til å videreformidle helseopplysninger til samarbeidende personell også utenfor virksomhetens grenser. Etter lovendring 19. juni 2009 nr. 68 fikk det helsepersonell som trenger opplysningene rett til å motta dem, med mindre pasienten motsetter seg det. Tidligere var slik videreformidling basert på at den som avgir opplysningene skulle vurdere om det var nødvendig.

[381] Dersom det skal etableres et virksomhetsovergripende, behandlingsrettet helseregister, begrenses typer opplysninger dette registeret kan inneholde. Hvis tilgang til opplysninger skal gis til personer som ikke er underlagt den databehandlingsansvarliges instruksjonsmyndighet, må adgangen til dette forskriftsfestes. Nærmere beskrivelse av disse relativt nye bestemmelsene følger nedenfor, i kapittel 5.2.2.

[382] Rett til innsyn i behandlingsrettede helseregistre, etter helseregisterloven § 22(1), gjelder så langt plikten til å gi slikt innsyn rekker i helsepersonelloven § 41. Innsynet kan begrenses i medhold av unntaksbestemmelser i pasientrettighetsloven § 5-1.

[383] Etter helseregisterloven § 26(5) gjelder også helsepersonelloven §§ 42–44 ved retting og sletting av helseopplysninger i behandlingsrettet helseregister. Disse bestemmelsene i helsepersonelloven tilfører blant annet krav til å nedtegne eventuelt avslag og begrunnelse for det i journalen, og rett til å klage over eventuelt avslag til Helsetilsynet i fylket.

[384] *EPJ Monitor. Årsrapport 2008. Oversikt over utbredelse og bruk av IKT i helsetjenesten*, s. 6 og 7.

herunder oppstille krav om opplæring og tiltak som skal sikre at utenforstående ikke får kjennskap eller tilgang til journalen.»[385]

Den helseinformatiske faglitteraturens, og de fagpolitiske dokumentenes, perspektiv på hva EPJ egentlig er, synes å være noe tvetydig. Tall for utbredelsen av EPJ har som utgangspunkt at dette forstås som et konkret programvareprodukt, med én leverandør og ett produktnavn. Slike produkter kan ha svært omfattende funksjonalitet, som i prinsippet kan dekke store deler av en helsetjenestevirksomhets behov, mens det i praksis er varierende hvor stor andel av dette IT-systemet som brukes aktivt i virksomheten.[386] En annen forståelse av hva EPJ er, ligger nærmere betraktningene om et «logisk registerbegrep». EPJ betraktes da som en logisk enhet der opplysninger fra ulike systemer, enheter og arkiver kan inngå.[387] Etter denne forståelsen kommer EPJ nærmere det å dekke hele definisjonen av behandlingsrettet helseregister. Med en slik innfallsvinkel blir EPJ et svært komplekst integrert informasjonssystem. Kompleksiteten kan i seg selv være krevende å håndtere, men det gir også klare fordeler ved at dokumentasjonsplikten kan ivaretas på forskjellige steder i det integrerte systemet. Alternativet, som er å forstå EPJ som et avgrenset produkt, innebærer at dette EPJ-produktet er det eneste IT-systemet virksomheten bruker for å ivareta dokumentasjonsplikten og oppfylle innholdskravene til en journal. Konsekvensen er at en rekke opplysninger må dobbeltføres eller kopieres fra ulike andre kliniske systemer til EPJ-produktet.

Dersom man velger den mer åpne tilnærmingen, et slags «logisk EPJ» der journalen forstås som virksomhetens informasjon om pasientene på tvers av ulike IT-systemer og eventuelle papirbaserte arkiver, kan det imidlertid oppstå et problem av en litt annen karakter. Rollen som journalansvarlig kan bli vanskelig å fylle.[388] En journalansvarlig vil trenge omfattende kunnskap om de ulike delene av det samlede informasjonssystemet, både for å vite hvilken informasjon det enkelte delsystem produserer, og for å forstå hvorvidt opplysningene fra ulike delsystemer ivaretar dokumentasjonsplikten godt nok eller ikke. Oppgaven med å «ta stilling til hvilke opplysninger som skal stå i pasientjournalen» vil uvegerlig også måtte innebære å ta stilling til hva som er den autoritative kilden hvis opplysningene i ulike IT-systemer ikke stemmer overens.

---

[385] Helsepersonelloven § 46.

[386] Rapporten *EPJ Monitor. Årsrapport 2008. Oversikt over utbredelse og bruk av IKT i helsetjenesten* bygger i hovedsak på en produktorientert forståelse av EPJ, uten at det står i veien for en betydelig interesse for integrasjon med andre kliniske systemer.

[387] En slik forståelse ligger bak definisjonen av EPJ i Nystadnes (2007a), s. 15: «Elektronisk ført samling eller sammenstilling av nedtegnede/registrerte opplysninger om en pasient i forbindelse med helsehjelp.»

[388] Jf. helsepersonelloven § 39(2): «I helseinstitusjoner skal det utpekes en person som skal ha det overordnede ansvaret for den enkelte journal, og herunder ta stilling til hvilke opplysninger som skal stå i pasientjournalen.» Pasientjournalforskriften bruker begrepet «journalansvarlig» om denne rollen.

En litt mer kuriøs problemstilling, som kan hefte ved perspektivet på EPJ som en sammensatt logisk systemintegrasjon, er hvorvidt det fører til at deler av EPJ vil måtte betraktes som medisinsk utstyr, med de skjerpede krav det innebærer, blant annet til CE-merking, kontroll og formell feilhåndtering med mer. Kravene til medisinsk utstyr er regulert av et EU-direktiv, som er implementert i norsk rett.[389] Ved en endring av direktivet i 2007 ble definisjonen utvidet slik at medisinsk utstyr også omfatter programvare i seg selv, dersom den brukes til diagnostiske eller terapeutiske formål.[390] Før denne endringen var programvare bare omfattet i den grad den var en del av annet medisinsk utstyr, og nødvendig for riktig bruk av dette utstyret på mennesker.[391] Det generelle svaret på et spørsmål om EPJ etter dette skal betraktes som medisinsk utstyr vil etter alt å dømme være nei.[392] Det utelukker likevel ikke at enkelte av de IT-systemer som kan inngå som delsystemer i en bred integrert, logisk EPJ kan tenkes å komme inn under definisjonen av medisinsk utstyr.

5.2.1.2 Pasientadministrative systemer (PAS)

Pasientadministrative systemer, PAS, er en betegnelse som brukes om et IT-system, eller funksjoner i et IT-system, for administrasjon av helsehjelp i en virksomhet. Slike funksjoner omfatter blant annet innleggelser og utskrivinger, henvisninger og innkallinger med videre. En plikt til å avgi bestemte opplysninger til pasientadministrasjon er et omfattende unntak fra helsepersonells taushetsplikt.[393] Det kan imidlertid være vanskelig å definere hva PAS er bare ved hjelp av det nokså åpne begrepet «administrativt». I praksis er det forskjeller fra virksomhet til virksomhet hvilke opplysninger de velger å plassere i PAS, og av hvilken årsak. Et eksempel er sykepleieres vaktskifterapport, som er i gradvis endring fra muntlige orienteringer til skriftlig dokumentasjon, som enkelte steder føres som relativt bredt tilgjengelig administrativ informasjon i PAS, og andre steder føres i EPJ.[394]

---

[389] Rdir 93/42/EØF.

[390] Formålet med endringen er omtalt i punkt 6 i fortalen til endringsdirektivet EP/Rdir 2007/47/EF: «Det er nødvendigt at præcisere, at software i sig selv er medicinsk udstyr, når det af fabrikanten er beregnet til en eller flere af de medicinske anvendelser, der er angivet i definitionen af medicinsk udstyr.»

[391] Denne endringen er gjennomført ved endringsforskrift 10. desember 2008, nr. 1352, ved at ordet «programvare» ble tilføyd i listen over typer gjenstander som er definert som medisinsk utstyr, i forskrift om medisinsk utstyr, 15. desember 2005 nr. 1690 § 1-5(1)(a).

[392] Den avgrensningen markeres i annet punktum i endringsdirektivets fortale punkt (6): «Software til generelle formål, der benyttes i forbindelse med sundhedspleje, er ikke medicinsk udstyr.»

[393] «Den som yter helsehjelp, skal uten hinder av taushetsplikten i § 21 gi vedkommende virksomhets pasientadministrasjon pasientens personnummer og opplysninger om diagnose, eventuelle hjelpebehov, tjenestetilbud, innskrivnings- og utskrivningsdato samt relevante administrative data.» helsepersonelloven § 26(2).

[394] Basert på to muntlige kilder, en av dem omtalte omleggingen til skriftlig dokumentasjon ved vaktskifte som «stille rapport».

Egne IT-systemer for pasientadministrasjon var på plass i mange sykehus før de fikk generelle EPJ-systemer. Etter hvert har det blitt mer vanlig at pasientadministrative funksjoner enten er inkludert i et EPJ programvareprodukt, som kombinert PAS/EPJ, eller at leverandøren av et EPJ-produkt også tilbyr et PAS-produkt som er designet for tett samspill med EPJ-produktet. En av grunnene til at man velger en tettere integrasjon mellom EPJ og PAS i sykehusene, er behovet for bedre kvalitet på opplysningene. Avvikende diagnosekoding mellom EPJ og PAS har, i følge rapporter fra undersøkelser av kodepraksisen, særlig hatt sammenheng med svake rutiner og metoder for å kontrollere endring av koder i PAS.[395]

PAS er, i likhet med EPJ, et behandlingsrettet helseregister etter helseregisterlovens definisjon. Det er nærliggende å betrakte PAS som en del av et «logisk EPJ», slik dette er beskrevet ovenfor. Da vil de pasientadministrative funksjonene, enten de finnes i et frittstående PAS, eller er nært integrert med eller direkte innlemmet i et EPJ-produkt, anses som et av de mange delsystemene som utgjør den samlede elektroniske journalen. En slik forståelse vil for så vidt være i strid med det Helse- og omsorgsdepartementet har uttalt, den gang pasientjournalforskriften ble vedtatt, om at pasientadministrative systemer ikke faller inn under begrepet journal.[396] Dette er imidlertid ikke et poeng som ser ut til å ha vært understreket eller fulgt opp senere, så det kan tenkes at tiden etter hvert har løpt fra den uttalelsen.

5.2.1.3 Avdelingsvise, kliniske informasjonssystemer (AKIS)

Betegnelsen AKIS, en forkortelse for avdelingsvise, kliniske informasjonssystemer, omfatter en rekke ulike IT-systemer som brukes i behandlingsrettet arbeid innen avgrensede medisinske fagdisipliner. AKIS er et slags analytisk begrep, som av og til brukes for å drøfte noen felles trekk og problemstillinger ved de fagspesifikke systemene, til tross for at dette egentlig langt fra dreier seg om noen ensartet gruppe IT-systemer. Om man skulle telle «antall IT-systemer» i et helseforetak, vil AKIS utgjøre den største gruppen.[397]

---

[395] Slike funn ble vektlagt både i Helsetilsynets rapport *Tilsyn med kodepraksis.* (2004) og i *Riksrevisjonens undersøkelse av kodekvaliteten ved helseforetakene*. Helse- og omsorgsdepartementet viser i sitt tilsvar i Riksrevisjonens rapport til at «de regionale helseforetakene arbeider med å koble elektronisk journal opp mot det pasientadministrative systemet. Dette vil forenkle kvalitetssikringen mellom pasientjournal og pasientadministrativt system.» (s. 11).

[396] Fra *Merknader til forskrift om pasientjournal*, publisert sammen med pasientjournalforskriften på Lovdata, merknad til forskriftens § 10.

[397] I en empirisk undersøkelse ved et av universitetssykehusene ble 60 slike systemer identifisert, og klassifisert etter en inndeling i ulike grupper bruksformål. Den største av disse gruppene, 19 systemer, var i stor grad journaldokumentasjon spesielt tilpasset den aktuelle avdelingens behov. Eivind Vedvik og Arild Faxvaag (2006): «The fate of clinical department systems at the dawn of hospital-wide electronic health records in a

Et av de fortrinnene man finner i en del av AKIS-ene er en mer velutviklet prosesstøtte, for de faglige oppgavene, enn man finner i generelle EPJ-produkter.[398] Spørsmålet om innlemming i eller integrasjon med EPJ er til dels det samme som for PAS. Ved manglende integrasjon vil det være behov for å duplisere opplysninger fra AKIS til den mer «offisielle» journalen. Man kan enten bevege seg i en retning som innebærer å erstatte ulike AKIS med funksjoner i EPJ som gir god nok prosesstøtte, med muligheter for å tilpasse systemet til ulike fagavdelingers behov, eller man kan satse på en systemintegrasjon der ulike AKIS er delsystemer i en «logisk EPJ».

En annen problemstilling i spørsmålet om samspill mellom EPJ og AKIS, er spenningen mellom styring og autonomi.[399] Uavhengig av om man velger å betrakte EPJ som et enkeltprodukt eller som en logisk sammenstilling av delsystemer, er det EPJ som fremheves som det viktigste systemet i den fremtidige elektroniske helsetjenesten. EPJ som et slags nav og hovedsystem er uttalt eller underforstått i dokumenter fra ulike typer premissgivere, både fra reguleringsmyndigheter og fra mange kunnskaps- og interessemiljøer.[400] Et autonomt AKIS gir det enkelte fagmiljø eierskap til og større grad av kontroll over sitt arbeidsverktøy. Arbeidet med å ta i bruk og tilpasse et generelt EPJ, som skal omfatte hele virksomheten er omfattende. Et utøvende, spesialisert fagmiljø kan oppfatte det generelle systemet som for kompromissorientert, i den forstand at konkret og nyttig prosesstøtte ofres for å oppnå mer samlet dokumentasjon. Alternativt kan fagmiljøer med interesser i et lokalt AKIS oppfatte sitt system som bedre skjermet mot en fare for at generelle styringshensyn skal diktere dokumentasjonen på bekostning av det de ser som faglige behov. Det kan også ligge en kilde til konflikt mellom EPJ og AKIS-interessenter i graden av informasjonsteknologisk profesjonalisering. Generelle EPJ utvikles og forhandles av eksterne leverandører, med stor kundeportefølje, og med krav til robusthet som kan føre til at systemendringer blir mer omstendelig og tungrodd. I et AKIS, som kan være mer amatørmessig som IT-produkt, kan fagmiljøet ha mer kontroll over systemendringer.

Norwegian university hospital». I: *Studies in health technology and informatics,* s. 298–303. Muntlige kilder har også nevnt atskillig høyere antall enn 60 AKIS ved enkelte helseforetak.

[398] Anders Grimsmo m. fl. (2007): «Prosesstøttende EPJ systemer – bakgrunn, definisjon og målsetninger».

[399] Kildesituasjonen er slik at omtaler av systemer i høy grad er innrettet etter fagpolitiske premissgiveres syn, det er derfor vanskelig å finne godt belegg for dette basert på litteratur. Resonnementer av samme slag som dette finnes imidlertid som en del av drøftingen i Vedvik og Faxvaag (2006).

[400] Dette er enten uttrykt konkret eller bygd inn som en forutsetning i det store flertallet av de kildene som det er henvist til her i kapittel 5.2.1.

5.2.1.4 Integreringsmåtenes betydning for tilgangskontrollen

Et helseforetak, eller annen institusjon i helsetjenesten av en viss størrelse, har et sammensatt behov for å behandle pasientopplysninger. I den relativt abstrakte gjennomgangen av noen typer informasjonssystemer ovenfor er det pekt på tre prinsipielt forskjellige innfallsvinkler til å styrke sammenhengene mellom disse. Disse tre innfallsvinklene må betraktes som mulige tendenser eller tankemodeller, det kan være adskillig flere momenter å stri med i reelle integrasjonsbestrebelser. Den ene innfallsvinkelen er å innlemme så mye som mulig i et generelt EPJ-produkt, fortrinnsvis for å utfase andre IT-systemer i størst mulig grad. Den andre er å definere EPJ som et virtuelt, eller logisk, system, der ulike IT-systemene betraktes som, og gjøres tilgjengelig som, den samlede journalen. Den tredje innfallsvinkelen er å rendyrke journalen som en form for bevismessig protokollføring for å kunne godtgjøre at «oss har gjort kva gjerast skulle», med det minimum av informasjon som dokumentasjonsplikten krever. Opplysninger som må være med i journalen vil da i en del tilfeller være en dublering av opplysninger som også kan finnes i andre IT-systemer, som ikke betraktes som del av journalen.

Hver av disse innfallsvinklene til integrasjon er det både mange fordeler og mange problematiske sider ved. Den betydningen det enkelte integrasjonsperspektiv har for tilgangskontrollen utgjør en temmelig beskjeden del av disse fordelene og ulempene, derfor er det neppe grunn til å legge avgjørende vekt på tilgangskontrollspørsmålene i valg av innfallsvinkel til integrasjon internt i en virksomhet.

Å innlemme så mye som mulig av behandlingen av helseopplysninger om pasientene i et konkret og avgrenset EPJ-produkt fører til at svært mange databrukere, som står mer eller mindre nær den helsehjelpen som ytes til den enkelte, får en potensiell mulighet for tilgang til helseopplysningene. Det å definere snevre nok tilgangskriterier, slik at de ligger nærmest mulig et samsvar med de konkrete behovene,[401] vil dreie seg om hvor presise kriterier det er mulig å uttrykke, og hvor god etterlevelse og oppfølging av kriteriene det lar seg gjøre å oppnå i dette enkeltstående men komplekse IT-systemet. Å samle alle kriterier og administrasjon av kriteriene i ett systemmiljø kan bidra til overskuelige effekter av de ulike kriteriene, og av eventuelle endringer i dem. På den annen side bidrar samlingen av et høyt antall databrukere og en stor mengde opplysninger til at små svakheter i tilgangskriteriene kan gi

[401] Jf. utgangspunktet for avhandlingens problemstilling: «Tilgang kan bare gis i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt», helseregisterloven § 13(1) annet punktum.

store utslag i form av databrukere som har mulighet for å få tilgang til opplysninger de ikke har behov for.

Forståelsen av EPJ som en logisk sammenstilling av delsystemer innebærer at relativt mange databrukere, men ikke alle, må ha tilgang til de fleste av delsystemene. Helseopplysningene befinner seg da i det enkelte delsystem, og ikke samlet i et felles EPJ-produkt. Det er imidlertid en mer begrenset mengde opplysninger i det enkelte delsystem, slik at den potensielle muligheten for tilgang er langt mindre enn kombinasjonen av alle databrukere og alle opplysninger. På den annen side vil det være behov for at langt flere databrukere gis tilgang til det enkelte delsystem enn det som er tilfellet med autonome AKIS som ikke betraktes som en del av den formelle journalen. Den utvidede kretsen av databrukere, som i mange tilfeller vil ha behov for tilgang til en begrenset andel av opplysningene i et delsystem, innebærer at det enkelte delsystem må underlegges de samme kravene til å kunne uttrykke og følge opp tilgangskriterier som de generelle EPJ-produktene. Logisk EPJ er et heterogent systemmiljø, som må underlegges et felles kontrollregime.

Den tredje innfallsvinkelen, minimumsjournal og autonome AKIS, er antakelig det bildet som ligner mest på dagens praksis i de fleste av helseforetakene. Det kan være uttrykk for lave ambisjoner om integrasjon mellom EPJ og fagsystemer. Alternativt, dersom ambisjonene er høye, kan det være resultatet av noe svak vilje eller evne til å gjennomføre integrasjon. I slike tilfeller vil det enkelte AKIS ha relativt få databrukere, fordi personer som ikke er helt direkte involvert i avdelingens aktiviteter vil finne opplysningene de har behov for i EPJ-produktet, som opplysningene er overført til.[402] Det konkrete problemet med å uttrykke tilganger tilstrekkelig presist synes å være mindre ved denne innfallsvinkelen. Derimot kan grensene mellom ulike autonome systemer bli uklar. Lignende, men ikke helt sammenfallende, behov for opplysninger dekkes flere steder. Det kan være vanskelig å opprettholde kunnskap om, og en etterprøvbar kvalitet i, den samlede mengden opplysninger. De problemene dette skaper for tilgangskontrollen er av mer indirekte karakter. Forutsetningen om at det i utgangspunktet er få spesialister som har behov for tilgang kan bli en sovepute for å akseptere svak differensiering av tilgangene i autonome delsystemer. Den forutsetningen kan imidlertid komme under press på grunn av vanskelighetene med å sikre kvaliteten i de opplysningene som ut fra

[402] Denne situasjonen er beskrevet slik i Ot.prp. nr. 51 (2008-2009), s. 23: «De høyt spesialiserte systemene benyttes primært av spesialister og inneholder i all hovedsak kun opplysninger som er nødvendige og relevante i forhold til den type helsehjelp spesialistene yter. Dette gjenspeiles gjerne i mekanismene for tilgangsstyring. Mulighetene for å differensiere tilgangen kan være svært begrenset. Enkelte system gir knapt noen slik mulighet, en bruker som fyller kravene for tilgang til en bestemt pasient, får tilgang til alt som er registrert om denne pasienten i det aktuelle systemet.»

dokumentasjonsplikten må inn i journalen. Resultatet blir at flere databrukere enn forutsatt opplever behov for tilgang til kildesystemene.

5.2.2 Behandlingsrettede helseregistre utover virksomhetsgrensene

Både tilgang til helseopplysninger i behandlingsrettede helseregistre som befinner seg hos en annen virksomhet, og det å etablere behandlingsrettede helseregistre på tvers av virksomhetsgrenser, er i hovedsak en kommende trend. Ved endringslov 19. juni 2009 nr. 68 ble det gitt ulike hjemler for slik samhandling.[403] Grunnprinsippet om at tilganger bare kan gis til de som står under den ansvarlige virksomhets instruksjonsmyndighet gjelder fremdeles, men kan etter lovendringen fravikes ved forskrift.[404] Denne muligheten for å gjøre unntak er dels en forutsetning for de ulike nye hjemlene for virksomhetsovergripende behandlingsrettede helseregistre som er omtalt i dette kapitlet. I tillegg kan det gjøres etter «sugerørsprinsippet», slik at helsepersonell ansatt i virksomhet A kan gis direkte tilgang til å slå opp i opplysninger om en pasient i et virksomhetsinternt helseregister i virksomhet B.[405]

Å utlevere helseopplysninger til en annen virksomhet er noe litt annet enn å gi tilgang eller å etablere registre på tvers av virksomheter. En utlevering innebærer at opplysningene kopieres fra et logisk helseregister til et annet. Både avgivende og mottakende virksomhet er databehandlingsansvarlig for sin egen behandling av helseopplysningene. Også før lovendringen som er omtalt ovenfor var det adgang til å utlevere opplysninger, med en rekke egne bestemmelser om dette, som gjelder fremdeles.

Med unntak av den første gruppen som omtales nedenfor i dette kapitlet, som kan kalles fagsystemer for undersøkelsesdata, er de anvendelsene som nevnes mer eller mindre på utviklingsstadiet, og kan vanskelig konkretiseres utover det å vise til hjemmelsgrunnlaget. I tillegg omtales en varslet nyskapning, en sentralisert såkalt kjernejournal.[406] Den siste, også litt åpne, gruppen anvendelser som omtales her er informasjonssystemer som involverer pasienten direkte i behandlingen av helseopplysninger. Dette er det rom for i lovverket, det

[403] Et uttrykk som brukes gjennomgående, både i forarbeider til endringsloven og i de endringene som ble vedtatt, er «virksomhetsovergripende». Det kan man ha både stilistiske og semantiske innvendinger mot, men det lar seg dessverre ikke velge bort i omtalen av disse bestemmelsene.

[404] Grunnprinsippet, jf. helseregisterloven § 13(1) første punktum hadde tidligere ingen unntaksbestemmelse. Med endringslov 19. juni 2009 nr. 68 ble det gitt adgang til å gjøre unntak fra dette i forskrift (2. ledd), med visse nærmere føringer: Det må innhentes uttrykkelig samtykke fra pasienten (3. ledd), men likevel slik at unntak fra krav til utrykkelig samtykke kan forskriftsfestes (4. ledd), og tilgangen kan bare gjelde oppslag i opplysninger om én pasient om gangen (5. ledd).

[405] Slik tilgang til andre virksomheters interne registre er behandlet i Ot.prp. nr. 51 (2008-2009), kapittel 7.

[406] Dette er et konkret tiltak i Stortingsmelding nr. 47 (2008-2009), der det varsles om at dette vil bli utredet med sikte på å komme tilbake med et lovforslag som hjemler et slikt system.

eksisterer i beskjedent omfang i praksis, og det er høyst sannsynlig at dette vil være en stigende trend. Utvikling i retning av pasienter som selv bruker, og bidrar med opplysninger i, informasjonssystemet handler antakelig i større grad om fagpolitiske valg og teknologisk modning enn om hjemmelsgrunnlag.

5.2.2.1 Utveksling, fagsystemer for undersøkelsesdata

Undersøkelsesdata fra ulike typer laboratorier, røntgenenheter og andre undersøkelsesenheter leveres fra relativt spesialiserte fagsystemer, så vel som organisatoriske enheter. Slike enheter finnes både som avdelinger innen et helseforetak og som selvstendige institusjoner som utfører undersøkelser og leverer svardata til bestillere i alle deler av primær- og spesialisthelsetjenesten. I likehet med AKIS-er er slike fagsystemer laget for smale og spesialiserte oppgaver. Til forskjell fra AKIS er de langt mer standardisert på tvers av organisasjoner innen samme fag. Overføring av laboratoriedata til ulike EPJ, først til allmennleger og etter hvert til sykehusene, ble utviklet og utbredt relativt tidlig.[407] Laboratorie- og røntgenvirksomheter var også relativt tidlig ute med muligheter for å overføre detaljert grunnlag for refusjonskrav til Rikstrygdeverket elektronisk.[408]

Overføring av røntgenbilder var en av pioneranvendelsene innen telemedisin.[409] Fagsystemer og organisatoriske enheter i denne kategorien er designet for å betjene mange bestillere av undersøkelser. Overføring av røntgenbilde er preget av at dette er systemer som overfører store datamengder, og at programvaren som brukes er standardisert internasjonalt.[410]

[407] Jf. omtale i *EPJ Monitor. Årsrapport 2008. Oversikt over utbredelse og bruk av IKT i helsetjenesten* s. 19: «På siste halvdel av 1980-tallet startet Fürst laboratorium elektroniske overføringer av laboratoriesvar til noen brukere av Infodoc og PROMED, og etter hvert for brukere av WinMed. Etter hvert ble Trygd–helsepostkassa en hovedkommunikasjonskanal i helsetjenesten. Fra begynnelsen av 1990 tallet er laboratoriesvar og legeregninger blitt overført elektronisk til legekontorene via denne kanalen.» (Produktnavnene det refereres til er ulike EPJ som er utbredt i primærhelsetjenesten). Senere har Norsk Helsenett overtatt som hovedkommunikasjonskanal i helsetjenesten.

[408] Jf. forskrift om stønad til behandling av lege m.v., 22. mai 2001 nr. 651, (Opphevet), kapittel IV (kapitlet var ikke inndelt i paragrafer): «Alle undersøkelser skal registreres i henhold til kodeverket NORAKO. Disse undersøkelseskodene skal overføres sammen med regningsidentifikasjon til Rikstrygdeverket. Det forutsettes bruk av LABRØNK og Kodeverk.» LABRØNK er et IT-system som ble utviklet av Rikstrygdeverket for å motta slike spesifiserte krav. Oppgaven ble overtatt av Helseøkonomiforvaltningen (Helfo) fra 2009.

[409] Om røntgen som telemedisinsk pioneraktivitet, se Gunnar Hartvigsen m. fl. (2007): «Challenges in Telemedicine and eHealth: Lessons Learned from 20 Years with Telemedicine in Tromsø» (konferanseartikkel).

[410] PACS/RIS er en standard og en produktkategori for systemer som formidler digital røntgen. PACS står for «Picture Archive and Communication System», og håndterer selve bildene. RIS står for «Radiology Information System» som håndterer booking av undersøkelser og registrering av svar.

5.2.2.2 Felles behandlingsrettet register i formaliserte arbeidsfellesskap

Det har over lengre tid utviklet seg en praksis der flere virksomheter har delt samme IT-system for føring av pasientjournaler. Denne praksisen har først og fremst dreid seg om kontorfellesskap, der selvstendige leger eller tannleger deler lokaler og en del fellesfunksjoner. I forarbeider til endringsloven 19. juni 2009 nr. 68 ble det betraktet som tvilsomt hvorvidt dette egentlig var tillatt, etter helseregisterlovens dagjeldende regler.[411] Derfor ble det foreslått, og vedtatt, en ny bestemmelse som hjemler forskrift om etablering av virksomhetsovergripende behandlingsrettede helseregistre for bruk av helsepersonell med formalisert arbeidsfellesskap.[412] Forskrift i medhold av den nye bestemmelsen skal sikre plassering av databehandlingsansvaret, og angi regler om tilgang og tilgangskontroll. Dersom et arbeidsfellesskap etablerer et virksomhetsovergripende behandlingsrettet helseregister, stilles det krav både om at registeret skal føres elektronisk og om at det virksomhetsovergripende registeret skal «erstatte det virksomhetsinterne behandlingsrettede registeret.»[413]

Den tydeliggjøringen av adgangen til slike registre som ble innført med den nye bestemmelsen i helseregisterloven virker etter alt å dømme fornuftig. Det kan imidlertid være grunn til å stille seg noe mer tvilende til proposisjonens korthugde anførsel om at dette ikke var tillatt før lovendringen. Et argument som taler mot at dette skal ha vært ulovlig tidligere er definisjonen av det logiske registerbegrepet. I den opprinnelige proposisjonen til helseregisterloven er dette beskrevet slik at det både kan dreie seg om å spre et register over flere datafiler, *og omvendt*, plassere flere registre på samme server.[414] En felles EPJ-installasjon som dekker flere selvstendige leger i samme legesenter skulle, ut fra denne begrepsbruken, kunne ses som ulike logiske registre i samme fysiske register. Det logiske registerbegrep er også omtalt i proposisjonen til endringsloven, men i den sammenheng nevnes bare den siden som dreier seg om at et register kan befinne seg i ulike elektroniske systemer og andre lagringsmedier. Den andre siden ved den opprinnelige tolkningen av begrepet, at flere logiske registre kan finnes i samme fysiske register, er gjenstand for en talende utelatelse.[415]

Et annet argument som kan tale mot den oppfatning at forskjellige leger i samme legesenter ikke kunne dele fysisk register før lovendringen, er en enstemmig kjennelse i Høyeste-

[411] Ot.prp. nr. 51 (2008-2009), s. 54. Gjeldende rett på området er fremstilt svært kort: «Tolkningen av §§ 6 og 13 i helseregisterloven gjør at man indirekte har et forbud mot etablering av virksomhetsovergripende behandlingsrettede helseregistre», med henvisning til tidligere redegjørelse for dette indirekte forbudet.
[412] Tatt inn i helseregisterloven, som ny § 6b. I proposisjonen antyder departementet at formalisert arbeidsfellesskap vil kunne favne noe videre enn bare rene kontorfellesskap. Noen få eksempler nevnes, men de kan ikke sies å tydeliggjøre noen yttergrense. Ot.prp. nr. 51 (2008-2009), s. 57.
[413] Helseregisterloven § 6b (3).
[414] Ot.prp. nr. 5 (1999-2000), s. 64. Også omtalt i kapittel 5.2 ovenfor.
[415] Jf. Ot.prp. nr. 51 (2008-2009), s. 18.

rett om hvorvidt en lege som avsluttet samarbeidet med et legesenter skulle ha anledning til å få med seg journalene fra senterets dataserver.[416] Legen som avsluttet samarbeidet fikk medhold i at hans pasienters journaler skulle følge med ham ut av legesenteret til ny praksis. Den primære begrunnelsen var at «taushetsplikten overholdes best ved at den som har taushetsplikt, også forvalter opplysningene. Dermed er det også tatt hensyn til pasientens behov.»[417] Begge parter i saken var enige i at dersom journalene skulle følge legen, måtte det også innebære at de skulle slettes fra legesenterets dataserver. Høyesterett løste spørsmålet etter helsepersonelloven, uten å komme direkte inn på verken helseregisterlovens registerbegrep eller den databehandlingsansvarliges ansvar og oppgaver.[418]

Et praktisk viktig moment som Høyesterett nevnte, men som de også gjorde klart at ikke hadde vært påberopt og heller ikke var gjenstand for prøving, var at en del av pasientene kunne ha vært behandlet av flere leger ved samme legesenter. Den typen problemstillinger er det rimelig å tro at vil melde seg også i andre tilfeller der deltakere går ut av og inn i formaliserte arbeidsfelleskap.[419]

5.2.2.3 Felles, behandlingsrettede helseregistre, mellom samarbeidende virksomheter

I endringsloven 19. juni 2009 nr. 68 ble det også gitt adgang til å etablere behandlingsrettede helseregistre med en del felles helseopplysninger som kan deles mellom samarbeidende virksomheter i helsetjenesten.[420] I likhet med felles system i et formalisert arbeidsfellesskap, stilles det krav om at også slike registre føres elektronisk, og at skal foreligge forskrift som regulerer databehandlingsansvar og regler om tilgang og tilgangskontroll med videre.

Formålet er imidlertid et annet. Virksomhetsovergripende behandlingsrettet helseregister mellom samarbeidende virksomheter er ment som et hjelpemiddel når flere virksomheter samarbeider, ut fra hver sin faglige spesialisering, om å tilby de samme pasientene behandling. Det er særlig to forhold som skiller slike registre fra de som etableres for et formalisert

[416] Rt. 2006 s. 1275.
[417] Rt. 2006 s. 1275, avsnitt 32.
[418] Høyesterett tar altså ikke konkret stilling til om den felles dataserveren skulle være i strid med helseregisterloven §§ 6 og 13. Resonnementene hviler imidlertid på en implisitt forutsetning om at journalene utgjør den enkelte deltaker i arbeidsfellesskapets «logiske register», altså samme tenkemåte som i utgangspunktet hadde ført til teoridannelsen «logisk register».
[419] Endringer i samarbeidskonstellasjoner er ikke direkte nevnt blant det som kreves av innholdet i en forskrift etter den nye § 6b i helseregisterloven. Det kunne kanskje likevel være hensiktsmessig å gjøre håndtering av slike endringer, på en måte som ivaretar pasientens interesser, til et tema i forskriften. Høyesteretts vurderinger viste blant annet til at det var lite veiledning å hente i pasientjournalforskriften § 15, som primært regulerer overtakelse av journal ved opphør eller overdragelse av virksomhet.
[420] Helseregisterloven § 6a.

arbeidsfellesskap.[421] Det ene er at det skal være et begrenset utvalg opplysningstyper i et slikt register. Hvilke opplysninger som kan inngå skal være basert på hva som er relevant for registerets formål. Nærmere angivelse av opplysningstyper fastlegges i forskrift. Den andre forskjellen er at «[s]like registre kan bare etableres i tillegg til de behandlingsrettede helseregistrene virksomheten etablerer internt i virksomheten.» Disse to momentene henger i en viss forstand sammen. Det er i praksis en forutsetning for å kunne avgrense mengden opplysninger i at behandlingsrettede helseregistre som skal støtte samarbeid mellom spesialiserte virksomheter at slike registre ikke får erstatte de virksomhetsinterne registrene.

Et sentralt, behandlingsrettet helseregister, med enkelte opplysninger som det kan ha stor betydning at er raskt tilgjengelige ved den virksomheten en pasient kommer til, kan i prinsippet betraktes som en utvidelse av klassen virksomhetsovergripende, behandlingsrettede helseregistre. Dette omtales som «nasjonal kjernejournal», er varslet som et svært aktuelt tiltak under utredning, og beskrives på denne måten:

> Begrepet nasjonal kjernejournal benyttes her om en IKT-basert løsning der helsepersonell som yter helsehjelp til en pasient kan, gitt autentisering og autorisasjon, få tilgang til et begrenset sett tilrettelagte *kjerneopplysninger* om pasienten. Med kjerneopplysninger menes *livbergende kritisk informasjon* (blodtype, allergier, etc.), gjeldende *medisinering* og *kontaktoversikt/epikriser*. En kjernejournal er *ikke* en journal, men en samling informasjon ekstrahert fra de elektroniske pasientjournaler (EPJ).[422]

Denne typen helseregister vil ha mye til felles med den typen virksomhetsovergripende registre som er nevnt ovenfor, der formålet er å støtte samarbeid om pasientbehandlingen mellom virksomheter. Den viktigste, og nærmest den eneste, forskjellen ligger i at den nasjonale kjernejournalen har et større nedslagsfelt, både geografisk og om man tar i betraktning hvor forskjelligartede virksomhetene som skal bruke registeret er.[423]

5.2.2.4 Egenjournal, e-helse og den aktive pasient

En alternativ strategi for å håndtere informasjonsbehovet ved samhandling mellom flere aktører i helsetjenesten, i stedet for felles registre, er å la pasienten besitte opplysningene selv, en såkalt egenjournal. En generell adgang til å etablere ordninger med egenjournal kom med

[421] Helseregisterloven § 6a (2).
[422] Stortingsmelding nr. 47 (2008-2009), s. 137.
[423] Helseregisterloven § 6a holder omfanget av slike registre litt åpent, men angir likevel en øvre grense: «Det kan ikke etableres sentrale behandlingsrettede helseregistre etter denne bestemmelsen», § 6a (3) tredje punktum. Dermed vil nasjonal kjernejournal kreve annen hjemmel, til tross for store likhetene mellom en slik kjernejournal og de registrene som § 6a hjemler.

helsepersonelloven, da den ble vedtatt.[424] Bakgrunnen var et representantforslag noen år tidligere,[425] oppfølgingen av forslaget ble av praktiske grunner lagt til arbeidet med ny helsepersonellov. I proposisjonen til helsepersonelloven var departementet gjennomgående positive til egenjournaler som et supplement, på avgrensede områder, men de mente samtidig at det også var «viktig å understreke at egenjournal ikke skal erstatte helsepersonellets generelle dokumentasjonsplikt, og at sammenblanding av egenjournal og pleieinstitusjoners medisinske opplysninger må unngås.»[426]

Det mest kjente og utbredte eksemplet på egenjournal i Norge er *Helsekort for gravide*, som svært mange kvinner har fått utlevert og båret med seg for å formidle opplysninger mellom ulike instanser i svangerskapskontrollen. Svangerskapsjournalen, som senere ble til Helsekort for gravide, var i stor grad drevet fram av fagmiljøet knyttet til Medisinsk fødselsregister. De så for seg, og argumenterte for, at opplysningene skulle være egnet for edb-registrering.[427] Den brede innføringen av svangerskapsjournal var imidlertid ikke i særlig grad rettet mot sentral innsamling av opplysninger, den dreide seg om konkret helsehjelp til den enkelte. I en bred utredning om helsehjelp under svangerskap og i tiden rundt fødselen, var en slik egenjournal, som den gravide selv medbringer til kontroller og til fødeinstitusjon, en av flere anbefalinger.

> En ordnet og oversiktlig opptegnelse av informasjonene om den gravide og svangerskapets utvikling er av stor praktisk betydning både som et arbeidsdokument og som et grunnlag for hensiktsmessige henvisningsrutiner og godt samarbeid. Det er derfor en fordel å benytte en egen svangerskapsjournal, som i tillegg kan tjene som grunnlag for en løpende evaluering av eventuelle tiltak under svangerskapet. … Kvinnen beholder originalen og første kopi under hele svangerskapet. De medbringes og oppdateres ved alle kontroller, ved henvisninger og ved innleggelse i fødeinstitusjon.[428]

Helsekort for gravide ble innført for å håndtere et praktisk informasjonsutvekslingsproblem, og ble ikke omtalt i samme type ideologiske vendinger om autonomi, eierskap og medvirkning som representantforslaget noen år senere var en slags opptakt til.[429]

---

[424] Helsepersonelloven § 39(3): «Departementet kan i forskrift pålegge helsepersonell som nevnt i første ledd å føre egen journal som pasienten oppbevarer selv (egenjournal).»
[425] Stortinget, *Dokument nr. 8:44 (1993-94)*.
[426] Ot.prp. nr. 13 (1998-1999), s. 124.
[427] Kjell Johansen og Leiv S. Bakketeig (1979): «Erfaringer med bruk av skjema for svangerskapskontroll». I: *Tidsskrift for Den norske lægeforening,* s. 389–391.
[428] NOU 1984:17, s. 34
[429] Et elektronisk helsekort for gravide er under prosjektering. Det ligger en viss ironi i at forprosjektrapportens anbefaling, i hvert fall for tidlige faser av dette systemet, vil redusere den gravides egen kontroll med opplysningene. Anbefalingen, blant flere vurderte alternativer, er en sentral, elektronisk samhandlingsløsning som utvikles trinnvis og som « … vil gi mulighet for å utvikle en webbasert løsning som gir den gravide tilgang når

Egenjournaler har også vært prøvd ut, og evaluert, i andre land enn Norge.[430] Et trekk som er felles for litteraturen på området er at den gjelder utprøving eller bruk i relativt begrenset omfang, og avgrenset til bestemte diagnoser eller behandlingsforløp. Egenjournaler har så langt ikke vært tatt i bruk for fullstendige, generelle pasientjournaler.

Senere har imidlertid flere ulike begreper vært lansert, som dreier seg om at pasienter får en mer aktiv rolle i håndteringen av helseopplysninger. Man finner dette omtalt som «e-pasienter», «praktiserende(!) pasienter», «pasient 2.0» med videre.[431] Et annet begrep som brukes er e-helse, og det er kanskje mer hensiktsmessig for denne avhandlingens emne fordi det i større grad dreier seg om et samlet bilde som både omfatter aktive pasienter, den elektroniske samhandlingen internt i helsetjenesten, og samhandling ut mot andre virksomheter. Samtidig er det mangesidige e-helsebegrepet i større grad de fagpolitiske premissgivernes arena, med den faren det kan innebære for en utvikling som favoriserer institusjonene på bekostning av den aktive pasients interesser. Innslaget av egenjournal, der pasienten bidrar og bestemmer, er ikke noe som i seg selv garanteres ved at pasienten kan logge seg på et nettsted. Spørsmålet om hvorvidt det kan være ønskelig eller ikke at pasienter bidrar som produsenter og kontrollører av egen journal har også vært drøftet som et medisinsk-faglig anliggende.[432] E-helse, og særlig pasientens rolle i dette, presenteres i stor grad som scenarioer, forventninger og målsetninger, men det finnes også konkrete eksempler.[433]

---

det eventuelt blir juridisk og politisk vilje.» Astrid Brevik Svarlien (2008): «Forprosjektet Elektronisk Helsekort for gravide (EHG) – Forslag til løsning og plan for hovedprosjekt», s. 28.

[430] Et eksempel på evaluering av et slikt forsøk, ved et sykehus i Skottland, finnes i Lisa Ritchie (2007): «Evaluation of a patient-held record for Meticillin Resistant Staphylococcus Aureus (MRSA)». I: *British Journal of Infection Control,* s. 25–29. I dette tilfellet var konklusjonen at både helsepersonell og pasienter fant egenjournalen akseptabel, men uten at det ble påvist klare forbedringer i kommunikasjonen.

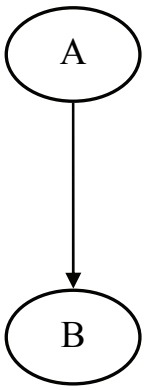
[431] Referanser som belegger fremveksten av disse og lignende begrepsdannelser ville bli høyst tilfeldige og ha liten hensikt. Det er summen av dette som viser en trend, en svært bred forventning fra mange hold om store endringer i samhandling og informasjonsbehandling mellom pasient og helsetjeneste.

[432] Jan C. Frich og Per Fugelli (2005): «Bør pasienten kunne skrive i egen journal?». I: *Tidsskrift for Den norske lægeforening,* s. 918. I denne debattartikkelen er forfatterne positive til det spørsmål de selv stiller, men peker samtidig på både kvalitet og ansvarsforhold som problematiske sider ved dette.

[433] Et eksempel er MinJournal: «MinJournal – på nett med helsevesenet»: *http://www.minjournal.no*, som er et samarbeid mellom flere helseforetak, med Oslo Universitetssykehus HF som databehandlingsansvarlig. Det er i moderat gjenge og under videreutvikling som en portal der pasienter, ved avdelinger som har tatt det i bruk, gis mulighet for å logge seg inn. Andre eksempler, fra store internasjonale aktører, er Microsoft® HealthVault, og Google™ Health. De to siste eksemplene er interessante fordi dette er pasientstyrte helseopplysninger som ikke er koblet til noen tilbyder av helsetjenester. I prinsippet gir dette pasienten full kontroll over samhandlingen, men uten at noen helsefaglig instans vil kunne ta ansvar for kvaliteten i opplysningene.

5.2.2.5 Hvilken betydning ulike muligheter for å bruke behandlingsrettede helseregistre på tvers av virksomhetsgrenser har for tilgangskontrollen

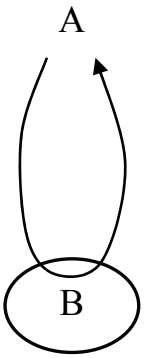
De ulike metodene for å bruke helseopplysninger i samhandling og samarbeid over virksomhetsgrensene har både en del felles og en del forskjellige konsekvenser for tilgangskontrollen. Flere av de nye bestemmelsene i helseregisterloven forutsetter at det vedtas forskrifter før adgangen til slik samhandling mellom virksomheter kan iverksettes.[434] Det er likevel mulig å utlede noen generelle og overordnede betraktninger ut fra gjennomgangen av de ulike metodene som er presentert ovenfor i dette kapitlet. En veldig enkel illustrasjon ledsager hver av de enkelte metodene som kan gi adgang til samhandling over virksomhetsgrenser. Tegnforklaringen er at hver oval er et behandlingsrettet helseregister, mens bokstavene A og B er to ulike virksomheter.



Figur 2: Overføring eller utlevering

Ved overføring eller utlevering av helseopplysninger, beholder hver av virksomhetene ansvar for sin egen bruk av opplysningene, i hvert sitt register som de er databehandlingsansvarlig for. A må ha sin berettigelse for å utlevere eller overføre det som A er ansvarlig for, B må ha sin egen berettigelse for å motta og innlemme opplysningene i sitt register. Autorisasjonene er imidlertid ikke gjenstand for noen felles forvaltning.

[434] Forskriftene som skal dekke dette er ikke gitt pr. 14. april 2010.



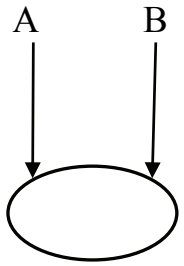
Figur 3: «Sugerørsprinsippet»

Med «sugerørsprinsippet», som er en tilgang til en annen virksomhets interne helseregister, må B kjenne til de aktuelle databrukerne fra virksomhet A, og vite hvilke autorisasjoner vedkommende har. Dette er i utgangspunktet en bilateral relasjon mellom to virksomheter. B forblir databehandlingsansvarlig, og må sørge for at det som er nødvendig av kontroll og oppfølging også omfatter de som kan ha tilgang utenfra. Det vil i praksis innebære et administrativt samarbeid der virksomhet A gir opplysninger om sine egne ansattes autorisasjon, og endringer i denne, til B.

I tillegg må A, på eget grunnlag, ha sin berettigelse for tilgang til de aktuelle opplysningene hos B.

Figur 4: Formalisert arbeidsfellesskap

I et formalisert arbeidsfellesskap er virksomhet A og B, som gjerne er to selvstendig næringsdrivende i et kontorfellesskap, databrukere i det samme behandlingsrettede helseregisteret. Databehandlingsansvaret må tilordnes, det mest aktuelle vil antakelig være at det tilordnes direkte til én av de deltakende virksomhetene. Den videre administrasjon, oppfølging og kontroll av de ulike deltakeres autorisasjoner, vil i praksis være omtrent som om dette var et virksomhetsinternt register. Denne modellen ligner på den situasjonen som ville gjelde for et kontorfellesskap av selvstendige aktører utenfor helsesektoren, dersom de har felles system og er omfattet av personopplysningsloven i stedet for helseregisterloven.



Figur 5: Felles register, samhandlende virksomheter

Et virksomhetsovergripende behandlingsrettet helseregister, som brukes av to eller flere virksomheter, kan befinne seg hos én av de deltakende virksomhetene, men både selve registeret og databehandlingsansvaret kan i prinsippet også plasseres andre steder. Ansvaret skal plasseres i medhold av forskrift. Opplysningene i registeret, som skal være avgrenset ut fra registerets formål, er imidlertid en felles ressurs som skal være like tilgjengelig for både A og B uavhengig av hvor registeret og ansvaret er plassert.

Innenfor disse generelle rammene kan det gis forskrifter som hjemler en relativt stor bredde av ulike samhandlingsmodeller. Innen feltet identitetsforvaltning, er det utviklet noe teori om samhandlingsmodeller for tilgangskontroll som kan tjene som utgangspunkt.[435] Den første modellen kan kalles en samarbeidsmodell, der initiativtakerne etablerer en styringsenhet som utvikler regler og avtalegrunnlag for de som skal delta. Denne modellen vil gi fleksibilitet til å håndtere en situasjon der ulike samarbeidsparter tilsluttes, og eventuelt trekker seg ut av samarbeidet om registeret. Styringsformen er indirekte, i den forstand at hver virksomhet autoriserer og overvåker sine databrukere i henhold til pålagte eller avtalte spilleregler for samarbeidet. Det er en viss fare for at det samlede nivået av sikkerhet blir lite overskubart, ettersom hver A og B kan ha forskjellig terskel for hvilken tillit de viser sine ansatte, eller for hvor mye som skal til før de iverksetter sanksjoner.

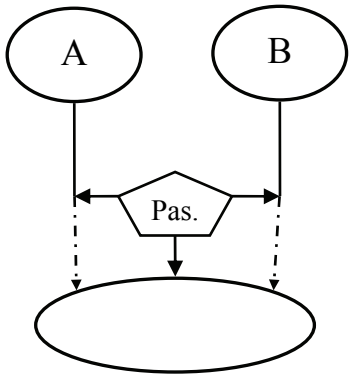
Den andre modellen er kalt konsortiummodellen, som er basert på at et lite antall initiativtakere etablerer et felles avtalt rammeverk, med noe grad av «suverenitetsavståelse» til konsortiet, på det området samarbeidet gjelder. Kontrollen med autorisasjonen blir mer direkte med denne modellen. Den er imidlertid lite fleksibel for utvidelser og endringer, både det å ta opp flere aktører og det å utvide registerets formål eller innhold kan være tunge prosesser som

[435] Identitetsforvaltning dreier seg primært om de aktivitetene innen tilgangskontroll som kan kalles administrasjon og autentisering, jf. kapittel 2.3. Modellene egner seg imidlertid også for denne avhandlingens problemstilling, samarbeid om å uttrykke og iverksette kriterier for autorisasjon. Betegnelsene på de modellene som beskrives er lånt fra Olsen (2009), s. 233–237.

krever mye av alle deltakerne i konsortiet. Modellen kan være velegnet for stabile samarbeidsrelasjoner, fortrinnsvis med relativt få deltakende virksomheter.

Den tredje modellen er en sentralisert modell. Den innebærer at det er én aktør som bestemmer reglene for samarbeidet. Graden av direkte eller indirekte styring kan varieres innen denne modellen, men det må forutsettes at den sentrale aktøren har en myndighetsrolle eller en noenlunde effektiv sanksjonsmulighet. De deltakende virksomhetene har prinsipielt liten innflytelse over spillereglene. Det er en robust modell, som tåler endringer både i deltakermassen og i tilgangskriteriene godt, men den er lite «lydhør» for lokale behov. Dersom man etablerer et virksomhetsovergripende behandlingsrettet helseregister i et regionalt helseforetak, som skal brukes til bestemte samarbeidsformål og som det gjøres obligatorisk for underliggende virksomheter å ta i bruk, vil antakelig en sentral modell være mest hensiktsmessig. En fremtidig, nasjonal kjernejournal bør antakelig også baseres på en sentralisert modell.

Den vide adgangen til å etablere virksomhetsovergripende behandlingsrettede helseregistre kan altså gi opphav til forskjellige modeller for å uttrykke og kontrollere databrukeres autorisasjon. Det vil i stor grad komme an på de forskriftene som vedtas hvor enhetlig eller forskjelligartet, direkte eller indirekte, lokal eller sentral tilgangskontrollen blir i praksis. Det er imidlertid fordeler og ulemper ved alle modellene. Resultatet for tilgangskontrollen blir antakelig best ved å velge ulike modeller for ulike typer registre og samhandlingsmønstre, fremfor å velge én standardisert modell for å følge opp alle former for tilgang på tvers av virksomheter.



Figur 6: Pasienten kontrollerer samhandlingen

Illustrasjonen til et oppsett for aktive pasienter, der pasienten kontrollerer samhandlingen, kan både inneholde elementer av en egenjournal som pasienten selv bidrar i, og et opplegg der pasienten selv bestemmer hvilke virksomheter eller enkeltpersoner i virksomheten som skal ha tilgang til felles ressurser. Pasienten kan imidlertid ikke gis direkte innflytelse over helse-

personells dokumentasjonsplikt.[436] En slik modell for pasientinnflytelse, og eventuelle varianter av dette, vil være en form for tilleggsservice til pasienten, utover de minstekrav som nåværende lovgivning stiller til helsetjenesten. Å legge til rette for mer aktive pasienter innebærer prinsipielt sett en styrking av pasientautonomien, men det vil neppe være forsvarlig å *erstatte* en robust tilgangskontroll i virksomhetene med et opplegg for pasientkontrollert samhandling. Kontrollen med tilgang og videreformidling må fungere også dersom pasienten ikke kan, eller ikke ønsker, å påvirke aktivt. Det bør også være grenser for hvor store konsekvenser av pasientens egne feil og misoppfatninger helsetjenesten skal kunne velge å finne akseptable.

5.2.3 Helseregistre som ikke er behandlingsrettede

At et helseregister ikke er behandlingsrettet betyr at det er ment å brukes til andre formål enn helsehjelp til pasienter. Det dreier seg imidlertid fremdeles om helseopplysninger, som i de fleste tilfeller har sitt utspring i en helsehjelpsituasjon. Ikke-behandlingsrettede helseregistre etableres for å ivareta en samfunnsinteresse, som i de fleste sammenhenger bare har sekundær nytteverdi for pasienten selv.

Selv om det ikke er en direkte definerende egenskap, har ikke-behandlingsrettede helseregistre i praksis ofte et større nedslagsfelt enn behandlingsrettede registre. At nedslagsfeltet er større innebærer ikke nødvendigvis et høyere antall pasienter, selv om det ofte er tilfellet. Dersom et helseregister er landsdekkende, men bare omfatter pasienter med en sjelden diagnose, vil det være et lite register med stort nedslagsfelt. Det har imidlertid ingen vesentlig prinsipiell betydning om det faktiske antallet pasienter er lavt. Helseregisterlovens opptrapping av kravene til berettigelse er knyttet til nedslagsfelt, hvorvidt det kreves samtykke, og i hvilken grad pasientene er identifisert i registeret.[437] Som et helt generelt utgangspunkt vil ikke-behandlingsrettede registre gjerne ha færre databrukere og et mer begrenset utvalg av opplysningstyper enn de fleste behandlingsrettede registre, men de vil omfatte en større populasjon av pasienter eller mulige, fremtidige pasienter.

Helseregisterloven angir i sin formålsbestemmelse tre hovedgrupper av formål. Den første gruppen dreier seg om helsehjelp, og dekkes av de nærmere bestemmelsene om behandlings-

[436] Dokumentasjonsplikten som sådan åpner ikke for pasientens direkte medinnflytelse. Pasienten kan imidlertid begjære korrigering, supplering eller sletting av gale mangelfulle eller belastende opplysninger, etter de reglene som gjelder for dette, jf. pasientrettighetsloven § 5-2 med videre henvisninger.
[437] Helseregisterloven angir i § 7 de grunnleggende vilkårene for etablering av regionale og lokale helseregistre, og i § 8 noe strengere vilkår for etablering av sentrale helseregistre.

rettede helseregistre. De to andre hovedgruppene av formål kan for enkelhets skyld benevnes administrasjon og forskning.[438]

Det administrative formålet der det er mest omfattende innsamling og bruk av helseopplysninger er finansierings- og refusjonsordningene. Det er først og fremst ordningen med innsatsstyrt finansiering av spesialisthelsetjenesten, som administreres av Helsedirektoratet, som er basert på bruk av et ikke-behandlingsrettet helseregister som er omfattet av helseregisterloven.[439] Beregningsgrunnlaget er detaljerte helseopplysninger som er innrapportert til Norsk Pasientregister.[440] Ulike refusjonsordninger som forvaltes av Helfo,[441] som delfinansierer primærhelsetjenesten og noen nærmere angitte typer institusjoner, er ikke omfattet av helseregisterloven til tross for at behandling av refusjonskrav forutsetter at helseopplysninger om den enkelte pasient rapporteres inn til et organ direkte underlagt Helsedirektoratet.[442]

Et formål som på et vis ligger implisitt i ulike finansierings- og refusjonsordninger, er å utøve kontroll med helsetjenesten.[443] Uvanlige mønstre, eller åpenbare feil i innrapporterte

---

[438] De to gruppene er ekstrahert fra den syntaktisk utfordrende setningen i helseregisterloven § 1(1) annet punktum: «Gjennom forskning og statistikk skal loven bidra til informasjon og kunnskap om befolkningens helseforhold, årsaker til nedsatt helse og utvikling av sykdom for administrasjon, kvalitetssikring, planlegging og styring.» En viss hjelp i tolkningen, og belegg for å se dette som to forskjellige hovedgrupper av formål, får man i lovens proposisjon, Ot.prp. nr. 5 (1999-2000), s. 177 og 183.

[439] Forkortes ofte ISF, og er basert på et besluttet vekttall for ulike diagnoserelaterte grupper (DRG). Tilordning til rett gruppe baseres på koder for hoveddiagnose, bidiagnose og behandlingsprosedyre. Dette utgjør 40 prosent av bevilgningene til de regionale helseforetakene, mens basisbevilgninger utgjør 60 prosent.

[440] Norsk Pasientregister har konkret lovhjemmel som sentralt, personentydig helseregister, helseregisterloven § 8(3)(8). Plikten til å rapportere inn til Norsk Pasientregister følger av § 9.

[441] Navn på et forvaltningsorgan, underlagt Helsedirektoratet. Navnet er avledet av *Helseøkonomiforvaltningen*.

[442] Dette fremgår av folketrygdloven § 21-11a: «Helseregisterloven får ikke anvendelse på behandling av personopplysninger i tilknytning til ytelser etter kapittel 5 med mindre annet framgår av helseregisterloven.» (femte ledd). «Ved behandling av saker etter kapittel 5 er Helsedirektoratet behandlingsansvarlig, jf. personopplysningsloven § 2 nr. 4, og har ansvaret for informasjonssikkerhet og internkontroll, jf. Personopplysningsloven §§ 13 og 14. Departementet kan i forskrift gi nærmere regler om behandlingsansvaret til Helsedirektoratet.» (sjette ledd).

[443] Bruk av sentral registrering i et IT-system for å kontrollere helsepersonell og pasienters adferd har en nærmest oppsiktsvekkende lang historie i Norge, helt tilbake til 1970. Som ledd i den nasjonale kontrollen med forskrivning av narkotiske stoffer etablerte Norsk Medisinaldepot, som på den tiden var et statlig grossistmonopol for legemidler, et system for detaljert kontroll med hvilke leger som skrev resepter på narkotiske stoffer til hvilke pasienter, og hvilke apoteker hver resept ble tatt ut. I en artikkel rettet mot norske leger (Bjørn Jøldal (1972): «Narkotikaforskrivning og forbruk i Norge». I: *Tidsskrift for Den norske lægeforening,* s. 1809–1811), er nærmest all vekt lagt på å forklare dette som en ordning for å avdekke og kontrollere pasienters misbruk. I en internasjonal artikkel, beregnet på lesere som fulgte med på FNs innsats mot narkotika, fremheves imidlertid også egnetheten for å kontrollere legene: «If a doctor's prescription habits seem to be unjustified or if there is reason to believe that he himself is an addict, a letter is first sent by the health authorities asking him for an explanation.» (Bjørn Jøldal og Tullik Halvorsen (1972): «Electronic data processing in the control of legal consumption of narcotics in Norway». I: *Bulletin on Narcotics (United Nations dept. of Social Affairs),* s. 55–57). Det var et omstendelig arbeid, ved utlevering av de aktuelle preparatene ble innholdet av hver enkelt resept tastet inn. Strengt tatt er dette en digresjon, men personidentifiseringen i dette tidlige regimet for kontroll med narkotika fra apotek var også interessant: Hver lege og hver pasient ble identifisert med fødselsdato, de to første bokstavene i fornavnet og de to første bokstavene i etternavnet. Det ble ansett som tilstrekkelig finmasket, men uten garanti mot lik identifikasjon av forskjellige individer. Årsaken til at dette ble valgt var at det den gang ikke var særlig vanlig at fødselsnummer fremgikk av legitimasjon, eller at folk husket sitt eget fødselsnummer.

opplysninger fra samme kilde, kan være en spore til å undersøke nærmere om det har rimelige forklaringer, skyldes kunnskapsmangel, svak kvalitetssikring eller bevisste omgåelser.

De administrative formålene har inntil nylig primært dreid seg om behovet for detaljerte helseopplysninger for å ivareta den overordnede samfunnsmessige styringen av helsesektoren. Det er imidlertid også gitt hjemler for, og under utvikling og igangsetting, ikke-behandlingsrettede helseregistre for konkret administrativ saksbehandling, som ikke er helsehjelp men som likevel involverer helseopplysninger om pasientene.[444]

Forskning er en mangfoldig gruppe av formål. En del registre er etablert som, og hjemlet som, rene forskningsregistre. Andre registre kan være behandlingsrettede, eller etablert for et administrativt formål, men likevel inneholde opplysninger som er attraktive for bruk i forskning.[445] Dersom forskning ikke er angitt som et formål med registeret, kommer de alminnelige bestemmelsene om formålsbestemthet og vilkår for å bruke opplysningene til andre formål, til anvendelse.[446] Et spesielt tilfelle, som sikrer at mange verdifulle opplysninger er tilgjengelig for forskning, er den dobbelte formålsangivelsen for Norsk Pasientregister. Hovedformålet er «å danne grunnlag for administrasjon, styring og kvalitetssikring av spesialisthelsetjenester», mens flere forskningsrelaterte formål er angitt å gjelde «i tillegg».[447] I proposisjonen til endringen i helseregisterloven som ble gjort for at Norsk Pasientregister skulle bli personentydig, er inndelingen i hovedformål og tilleggsformål begrunnet slik:

> I utgangspunktet bør registre inneholde de opplysninger som er relevante og nødvendige for å ivareta sine formål. Departementet mener imidlertid at innholdet i NPR ikke skal defineres ut fra hvilke opplysninger som er mest nyttig for forskningsformål, da dette kan medføre at registeret får et datasett som blir mye større enn i dagens register. … Departementet mener derfor at administrasjon, styring og kvalitetssikring av helsetjenester skal være et hovedformål for et personidentifiserbart register. Dette var også forslaget i forskriftsutkastet som var på høring. Når dette defineres som et hovedformål innebærer det at det i utgangspunktet skal være bestemmende for hvilke sensitive opplysninger som kan registreres i registeret. Konstruksjonen med hoved-

[444] Her siktes det til to slike hjemler: *Nasjonal database for elektroniske resepter*, helseregisterloven § 8(3)(9), er en sentral kjerne i et større saksbehandlingsopplegg for elektroniske resepter, som omfatter forskrivingsstøtte, ekspedering og oppgjør, der ulike aktører har sine delsystemer som samhandler elektronisk med denne kjernen. Den andre er § 6c, om saksbehandling av frikort og refusjon av egenandeler, og administrasjon og samordning av pasienttransport. I det siste tilfellet ble informasjonssystemet etablert uten at databehandlingsansvar og hjemmelsgrunnlag var tilstrekkelig klart, lovendringen kom etter at svakheten var påpekt blant annet av Datatilsynet, jf. rapporten *Sviktende tilgangsstyring i elektroniske pasientjournaler? Lovforslag om å tillate direkte tilgang til pasientjournaler på tvers av virksomhetsgrensene* (2009).

[445] At egnede opplysninger finnes er imidlertid ikke tilstrekkelig for å bruke dem til forskningsformål, det stilles også krav til at forskningsprosjektet må være forhåndsgodkjent av den regionale komiteen for medisinsk og helsefaglig forskningsetikk, jf. helseforskningsloven § 9.

[446] Jf. helseregisterloven § 11.

[447] Norsk pasientregisterforskriften § 2.

> formål vil innebære en juridisk skranke for at registeret eser ut slik Datatilsynet er bekymret for.[448]

Denne begrunnelsen peker, riktignok indirekte, på et spesielt trekk ved helseregistre som har forskning som formål. Mens de administrative formålene lar seg avgrense til bestemte og forhåndsdefinerbare opplysningstyper, er det vanskeligere å sette grenser for hvilke opplysningstyper som har en potensiell, fremtidig nytte i forskningen. Opplysningene har verdi som en mulig kilde til ny kunnskap. Hvem som kan ha nytte av opplysningene, og til hva slags forskningsprosjekter, er det vanskelig å forutse fullt ut.

En måte å klassifisere helseregistre til forskningsformål på, er å skille mellom sentrale helseregistre og medisinske kvalitetsregistre.[449] Et sentralt helseregister har som regel en egen forskrift som avklarer nærmere hvem som er ansvarlig, hva registeret inneholder og hva det skal brukes til. Medisinske kvalitetsregistre er oftest knyttet til en spesifikk diagnose eller en bestemt type behandling, og brukes til å systematisere erfaringene med behandlingen. Både sentrale helseregistre og medisinske kvalitetsregistre aggregerer helseopplysninger over tid. Historisk sett har de sentrale helseregistrene vært etablert og forvaltet av epidemiologiske forskningsmiljøer, mens kvalitetsregistrene har vært etablert med nærmere tilknytning til kliniske miljøer, ofte initiert av behandlende helsepersonell. De medisinske kvalitetsregistrene er oftest basert på pasientens samtykke, mens sentrale helseregistre ofte har en hjemmel som angir at registrering kan skje uten samtykke.[450]

Et enkeltstående forskningsprosjekt kan også generere sin egen samling av helseopplysninger, for det aktuelle prosjektets egne formål. Det vil i så fall ikke være omfattet av helseregisterlovens bestemmelser.[451]

5.2.4 Helseopplysninger utenfor helsetjenesten og helseforvaltningen

I en del tilfeller har helsepersonell rett til, og i andre tilfeller plikt til, å videreformidle helseopplysninger til aktører utenfor helsetjenesten og helseforvaltningen. En opplysningsrett er et

[448] Ot.prp. nr. 49 (2005-2006), s. 31.
[449] Dette skillet er blant annet beskrevet i strategidokumentet *Gode helseregistre – bedre helse* (2009), s. 25, der det uttalte strategiske målet er å oppnå en teknologisk og organisatorisk konvergens av de ulike registertypene.
[450] Bildet er kanskje i ferd med å endre seg noe. Ved endringslov 9. april 2010 nr. 14 besluttet Stortinget at et nasjonalt register over hjerte- og karlidelser, som er et medisinsk kvalitetsregister nært til den kliniske behandlingen, kan etableres som personidentifiserbart register uten å baseres på samtykke fra pasientene.
[451] Forskningsprosjektet må være forhåndsgodkjent av den regionale komiteen for medisinsk og helsefaglig forskningsetikk, og det er etter helseforskningsloven § 33 et «nødvendig og tilstrekkelig behandlingsgrunnlag for helseopplysninger i medisinsk og helsefaglig forskning.» Det er personopplysningsloven, og ikke helseregisterloven, som gjelder som utfyllende bestemmelser til helseforskningsloven.

unntak fra taushetsplikten som helsepersonell har anledning til å benytte seg av.[452] En plikt vil i denne sammenheng innebære at helsepersonellet ikke selv kan ta stilling til behovet, og at videreformidlingen ikke er avhengig av samtykke fra pasienten.[453]

Bruken av helseopplysninger til ulike formål utenfor helsesektoren kan i seg selv betraktes som et problem, fordi volumet av denne bruken er vanskelig å få oversikt over. Det har vært pekt på at faren for stor spredning av helseopplysninger kan gjøre pasientene mer tilbakeholdne med å gi opplysning til helsetjenesten i utgangspunktet, slik at det også til syvende og sist kan være et medisinsk problem.[454]

Plikt eller rett til å gi helseopplysninger til aktører utenfor helsetjenesten og helseforvaltningen vil som regel være avgrenset av relativt smale formål, som innebærer stramme grenser for hva mottakende virksomhet kan bruke opplysningene til. Det er imidlertid andre sider ved reguleringen enn formålsbestemtheten som gjør videreformidling utenfor sektoren mindre overskubar enn innenfor sektoren. Et forhold som kan nevnes, selv om det formodentlig er av mer beskjeden betydning, er at helseopplysningene da er utenfor helseregisterlovens virkeområde.[455] Et forhold som derimot vil kunne ha store konsekvenser er forskjeller i taushetspliktens grunnleggende innretning. Taushetsplikt etter helsepersonelloven er yrkesmessig, eller personlig. I det meste av annen offentlig virksomhet er taushetsplikten organintern, slik at den som videreformidler opplysningene til et forvaltningsorgan ikke påvirker hvilke enkeltpersoner i organet som skal ha tilgang til dem.[456] En organintern taushetsplikt innebærer ikke et fravær av krav til tilgangskontroll hos de virksomhetene som behandler helseopplysninger og andre personopplysninger. Man har imidlertid ikke en like sterk føring om at det skal være samsvar mellom tilgangskontrollen og den enkelte databrukers taushetsplikt hos politi, sosialtjeneste, Nav eller forsikringsselskap med videre, som i helsetjenesten og helseforvaltningen.

---

[452] I de fleste tilfeller vil dette dreie seg om å gi opplysninger når pasienten samtykker til det, etter helsepersonelloven § 22, for eksempel i forbindelse med saksbehandling av velferdsytelser eller premiefastsettelse hos et forsikringsselskap. Opplysningsrett for helsepersonell kan også være uavhengig av samtykke, et eksempel er adgangen etter § 28 til å gi opplysninger om en arbeidstakers helseforhold videre til arbeidsgiveren, i den grad opplysningene gjelder arbeidstakerens skikkethet til et bestemt arbeid eller oppdrag.

[453] Et av eksemplene på en slik plikt er at helsepersonell av eget tiltak skal melding til barneverntjenesten når det er grunn til å tro at et barn blir mishandlet eller utsatt for alvorlig omsorgssvikt, helsepersonelloven § 33(2). I vilkåret «grunn til å tro» ligger det et rom for faglig skjønn, men det er likevel ikke anledning til å la være å melde fra dersom dette vilkåret er oppfylt. Helsepersonell skal også gi opplysninger til barneverntjenesten om de får pålegg om det (tredje ledd). Et annet eksempel er plikten etter § 31 til å varsle politi og brannvesen dersom dette er nødvendig for å avverge alvorlig skade på person eller eiendom.

[454] Blant annet er dette resonnementet presentert i Anders Grimsmo (2007): «Medisinskfaglig analyse av behovet for enklere kommunikasjon i tilknytning til bruken av elektronisk pasientjournal», s. 6, med belegg fra flere utenlandske studier som viser dette.

[455] Betydningen av dette er formodentlig beskjeden, fordi det da vil være personopplysningsloven eller annen spesiallov om behandling av opplysninger som sikrer plassering av ansvar og som pålegger den ansvarlige visse grunnleggende plikter, blant annet til å ivareta informasjonssikkerheten.

[456] Begrepene yrkesmessig og forvaltningsmessig taushetsplikt behandles mer detaljert i kapittel 6.3.2.1.

6 Helseopplysninger som gjenstand for regulering

Et utgangspunkt for å beskrive regler og metoder for å beskytte helseopplysninger, er å se på forskjellen mellom helsehjelp og helseopplysninger. Helsehjelp er ulike sider ved å legge til rette for og gjennomføre medisinsk behandling.[457] Helsepersonell har plikt til å utøve helsehjelp på en måte som er forsvarlig, og en plikt til å gi øyeblikkelig hjelp i situasjoner der det er nødvendig.[458] Den medisinske behandlingen vil som utgangspunkt, og også helt konkret i mange situasjoner, være et legemsinngrep.[459] Det ytterste mål for regulering av og kontroll med helsehjelp er å beskytte pasientens fysiske integritet.

Helseopplysninger, i dokumentert form, som forvaltes av helsetjenesten og andre som får tilgang til dem, er et produkt av helsepersonells plikt til å dokumentere helsehjelpen. Behovet for å beskytte helseopplysningene er imidlertid ikke begrenset til det fysiske medium som helsepersonellet først nedtegner dokumentasjonen på. Beskyttelsesbehovet er knyttet til at opplysningene ved å dokumenteres på et vis kobles fra helsehjelpen, kan brukes om igjen, tolkes på nytt, videreformidles til andre, inngå som grunnlag i beslutninger, bli en del av pasientens biografi og selvbilde. Det er primært opplysningenes immaterielle dimensjon, og ikke den fysiske representasjonen, som er gjenstand for et reguleringsbehov.

Frakobling fra den umiddelbare helsehjelpen foregår ikke bare når opplysningene formidles videre til andre formål enn helsehjelp. Dokumenterte helseopplysninger har allerede begynt å leve sitt eget liv idet de leses på nytt og brukes som bakgrunnskunnskap i nye konsultasjoner hos samme eller annet helsepersonell. En beskrivelse som fanger opp dette finner man i en kommentar som Aaslestad gir til sin boktittel *Pasienten som tekst*. Som et lån fra lingvistiske tekstfortolkningsmetoder, har det også i samfunnsvitenskaper blitt relativt vanlig å tolke et fenomen som om det var en tekst. De som forholder seg til fenomenet er

[457] «Med helsehjelp menes enhver handling som har forebyggende, diagnostisk, behandlende, helsebevarende eller rehabiliterende mål og som utføres av helsepersonell», helsepersonelloven § 3(3).
[458] Helsepersonelloven §§ 4 og 7.
[459] Henriette Sinding Aasen (2000): *Pasientens rett til selvbestemmelse ved medisinsk behandling*.

lesere, eller eventuelt skrivere, av denne teksten. I slike sammenhenger blir uttrykket «som tekst» en metafor, slik at for eksempel møtet mellom lege og pasient kan tolkes med de lingvistiske begreper og metoder som brukes for å tolke møtet mellom leseren og en tekst. Boktittelen *Pasienten som tekst* omfatter imidlertid noe mer enn denne metaforen. Det som står i journalene kan hentes frem igjen, og inngå i en hermeneutisk forståelse av pasienten.

> Legen (leseren) møter pasienten (teksten). Men legen møter også, og tar stilling til, i nær sagt alle medisinske konsultasjoner, unntatt «det første møtet», *teksten om pasienten.* Og denne teksten utgjør en ikke uviktig del av pasienten i det videre. «Pasienten» vil altså i mange tilfeller rett og slett være tekst.[460]

Det er disse immaterielle sidene ved helseopplysningene som er bakgrunnen for regulering av og kontroll med helseopplysninger. Helsehjelp og helseopplysninger berører dermed to forskjellige sider ved pasientens integritet.[461]

6.1 Helseopplysninger innen personopplysningsretten og helseretten

Regulering av og kontroll med helseopplysninger er et tema som står relativt sentralt i både helseretten og personopplysningsretten.[462] De krav man må, bør, eller kan stille til kontrollen med tilgang til og videreformidling av helseopplysninger, vil bygge på både detaljregler og mer generelle trekk ved disse to rettsområdene.

Personopplysningsrett omhandler vilkår for og krav til behandling av personopplysninger generelt. Helseopplysninger er en del av personopplysningsretten, som er avgrenset etter opplysningenes innhold. Personopplysningsretten har direkte å gjøre med den immaterielle dimensjonen ved vern av privatsfæren. Det har vært, og er fremdeles, vanlig å bruke begrepet personvern om personopplysningsrettens emne. Etter hvert har det imidlertid også blitt vanlig å presisere emnet til person*opplysnings*vern. Denne begrunnelsen er fremdeles dekkende:

---

[460] Aaslestad (2007), s. 196 (original utheving og tegnsetting).

[461] En slik forskjell i beskyttelsesbehovene for det fysiske og det immaterielle gjelder generelt for privatsfæren, ikke bare for forskjellen mellom helsehjelp og helseopplysninger. Jf. for eksempel Are Stenvik (2003): «Rettsbeskyttelse av personlig særpreg». I: *Tidsskrift for Rettsvitenskap,* s. 601–647: «Privatsfæren kan sies å ha både en fysisk og en immateriell dimensjon. Den immaterielle dimensjonen omfatter privat og personlig *informasjon*. Slik informasjon er det normalt like stort behov for å beskytte om den befinner seg utenfor den fysiske privatsfære, f.eks. om den er nedtegnet i en sykejournal eller innført i et offentlig register, som om den hadde ligget nedlåst i en skuff innenfor hjemmets fire vegger» (s. 605, original utheving).

[462] Som et analytisk grep vurderes deler av disse to rettsområdene som er relevante for regulering av helseopplysninger i første omgang atskilt fra hverandre. Deretter drøftes noen likheter og forskjeller. Dette valget av fremstillingsmåte er kanskje litt ukonvensjonelt, og begrunnes nærmere i kapittel 6.1.1 nedenfor.

> I artikkelen her nytter jeg termen 'personopplysningsvern' om den delmengde av begrepet 'personvern' som gjelder vern av personopplysninger. Termen 'personvern', som ble lansert på 1970-tallet for å aksentuere den rettslige betydningen av å skille mellom 'integritetsbeskyttelse' og 'vern av personopplysninger', har – dessverre? – blitt så populær *også* utenfor de kretser som lanserte termen, herunder i rikets høyeste domstol, at den titt og ofte brukes som synonym for 'injurievern' og 'integritetsbeskyttelse'. Dermed har termen mistet sine fortrinn – og rettsvitenskapen må ta i bruk nye termer for å gjenopprette presisjonen i problemtilnærmingen.[463]

Personvernkommisjonen omfavnet også denne presiseringen av begrepet, og tok i sin rapport tar til orde for å formalisere skillet mellom personvern og personopplysningsvern.[464]

På det personopplysningsrettslige område utgjør EUs personverndirektiv, i hovedsak implementert ved helseregisterloven, den generelle personopplysningsloven og personopplysningsforskriften, det grunnleggende regelverket om behandling av helseopplysninger.[465] Helseregisterloven legger generelt noe strengere føringer for behandling av helseopplysninger enn den generelle personopplysningsloven.[466] Helseregisterlovens virkeområde er grunnleggende sett institusjonelt avgrenset, den gjelder for behandling av helseopplysninger i helsetjenesten og helseforvaltningen.[467] Helseopplysninger som behandles utenfor denne institusjonelle avgrensningen, for eksempel i velferdsforvaltningen, i forsikringsselskap eller hos arbeidsgiver, er omfattet av den generelle personopplysningsloven. Et eksempel der den institusjonelle avgrensningen er fulgt til punkt og prikke, er reguleringen av alternativ behandling.[468] Forholdet til helseregisterloven og personopplysningsloven er ikke nevnt i selve loven, man må derfor se hen til helseregisterlovens og personopplysningslovens egne angivelser av virkeområde. Forskjellen er tilsiktet, og omtalt slik i proposisjonen:

> Dersom alternativ behandling gis innenfor helsetjenesten, vil helseregisterloven og helselovgivningens dokumentasjonsregler komme til anvendelse. For alternativ behandling som gis utenfor helsetjenesten og som ikke gis av autorisert helsepersonell, vil det være personopplysningsloven som regulerer i hvilken grad og på hvilke vilkår det er adgang til å behandle helse-/personopplysninger.[469]

---

[463] Jens Petter Berg (1999): «Personopplysningsvern i et nytt årtusen – kritikk av personopplysningslov-proposisjonen». I: *Kritisk Juss,* s. 351–377. (s. 353, original utheving).
[464] Mens «personvern dreier seg om ivaretakelse av personlig integritet», dreier personopplysningsvern seg om «regler og standarder for behandling av personopplysninger som har ivaretakelse av personvern som hovedmål.» NOU 2009:1, s. 32.
[465] EP/Rdir 95/46/EF, helseregisterloven, personopplysningsloven og personopplysningsforskriften.
[466] Det konkrete eksemplet på dette som er av størst betydning her, er kravet til samsvar mellom tilgangskontroll og gjeldende bestemmelser om taushetsplikt, helseregisterloven § 13(1) annet punktum, som er utgangspunkt for avhandlingens problemstilling.
[467] Helseregisterloven § 3.
[468] Alternativ behandlingsloven, 27. juni 2003 nr. 64.
[469] Ot.prp. nr. 27 (2002-2003), s. 63.

Det finnes i tillegg noen få eksempler på situasjoner der det er truffet konkret beslutning om hvilken lov som skal gjelde, uavhengig av det institusjonelle kriteriet. Dette har vært gjort begge veier. Helseregisterloven gjelder for Forsvarets helseregister, selv om det behandler helseopplysninger utenfor helsetjenesten og helseforvaltningen.[470] Personopplysningsloven gjelder for behandling av refusjonskrav i Helfo, selv om virksomheten hører til under helseforvaltningen.[471] Dessuten gjelder personopplysningsloven som utfyllende bestemmelser til helseforskningsloven, selv om en betydelig andel av forskningsprosjektene som godkjennes etter denne loven vil gjennomføres av virksomheter i helsetjenesten og helseforvaltningen.[472]

Mens personopplysningsretten har behandling av opplysninger som sitt hovedanliggende, dreier helserett seg primært om forsvarlig helsehjelp. Behandling av opplysninger er et underordnet emne, selv om også det er gjenstand for en rekke bestemmelser. En måte å systematisere helseretten på, er en inndeling av reglene i fem tematiske hovedgrupper, knyttet til henholdsvis helseinstitusjonene, sykdommene, legemidlene, helsepersonellet og pasientene.[473] Regler om behandling av helseopplysninger er i større eller mindre grad en underordnet del av alle de fem hovedgruppene, men kanskje tydeligst til stede i helsepersonellets plikter og pasientenes rettigheter. Helseretten omfatter mange, både konkrete og mindre konkrete, bestemmelser om behandling av helseopplysninger. Det gjelder først og fremst den generelle taushetsplikten, med en rekke ulike unntak, dokumentasjonsplikten, pasienters innsynsrett og en viss grad av rett til medbestemmelse.

Personopplysningsrettslige regler om behandling av opplysninger er i hovedsak knyttet til den virksomhet som er ansvarlig for behandlingen. I helseretten ligger virksomhetens ansvar for behandling av opplysninger mer i bakgrunnen, som en del av et sørge-for ansvar, mens de konkrete pliktene er plassert hos det enkelte helsepersonell.[474] Denne forskjellen har både prinsipielt og praktisk relativt stor betydning. Virksomhetens plikter dreier seg om å treffe

[470] I medhold av helseregisterloven § 3(3) kan Kongen i Statsråd bestemme i forskrift at loven skal gjelde utenfor helsetjenesten og helseforvaltningen. Forskrift om forsvarets helseregister, 2. september 2005 nr. 1010 knytter i en rekke bestemmelser registeret til helseregisterloven, blant annet ved at Forsvarsdepartementet er *databehandlingsansvarlig,* jf. forskriftens § 1-5.

[471] Folketrygdloven § 21-11a (5) og (6). Dette var oppgaver som Helfo, underlagt Helsedirektoratet, overtok fra Nav, tidligere trygdeetaten, 1. januar 2009. Departementet argumenterte for å videreføre dette som behandling regulert av personopplysningsloven, ut fra en formålsbetraktning, selv om det brøt med Helseregisterlovens institusjonelt avgrensede virkeområde: «Opplysningene og behandlingen av disse endrer ikke karakter etter overføringen av helserefusjoner til Helsedirektoratet – det er fremdeles tale om forvaltning av trygdestønader», Ot.prp. nr. 82 (2007-2008), s. 3.

[472] Helseforskningsloven § 2(3), jf. helseregisterloven § 3(4).

[473] Kjønstad (2007), s. 23–24.

[474] Det finnes imidlertid enkeltbestemmelser som går et stykke i retning av å peke på virksomheten. I forbindelse med helsepersonells plikt til å melde visse situasjoner til barnevernet, trekkes helseinstitusjonen inn på denne måten: «I helseinstitusjoner skal det utpekes en person som skal ha ansvaret for utleveringen av slike opplysninger.» Helsepersonelloven § 33(4).

tiltak basert på generelle vurderinger og tolkninger, mens helsepersonells plikter er mer rettet mot håndteringen av hver enkelt situasjon. Resultatet av for dårlig arbeid fra virksomhetens side er systematiske svakheter i behandlingen av opplysninger, som kan ha konsekvenser for mange, mens helsepersonell som misforstår eller bryter regler står i fare for å begå overtramp med store konsekvenser for enkeltpasienters personopplysningsvern.

Selv om helseretten i seg selv har omfattende regler om vern av helseopplysninger, vil en helserettslig premiss være at opplysningene er et slags biprodukt av helsehjelpen. Personopplysningsrettslige regler og oppfølgingsregimer har sitt utgangspunkt i et selvstendig vern av opplysningene som holder stand også når de kobles fra den helsehjelpen som ga opphav til opplysningene.

6.1.1 Et valg om en komplementær lesning av de to rettsområdene i avhandlingen

Både personopplysningsrett og helserett er relativt unge navn på rettsområder. De har likevel rukket å bli ganske godt etablert, med egne spesialister, undervisningstilbud, og norsk og internasjonal faglitteratur. Felles for personopplysningsrett og helserett er at de er mer knyttet til de fenomenene som reguleringen gjelder enn til etablerte rettslige grunnbegreper.[475] Det fører nødvendigvis i seg selv til overlapping med andre betegnelser på rettsområder.

Rettsområder, som middel til å strukturere tenkning og praksis, er egentlig merkverdig lite problematisert. Det kan skyldes at rettsområder har liten formell tyngde, man påberoper seg ikke en kobling mellom et argument og navnet på et rettsområde som et tolkningsmoment. Som spesialiserte faglige enklaver kan imidlertid en rettsområdeinndeling tenkes å få stor uformell tyngde.[476] I rettsvitenskapelige oversiktsverk, kursoversikter, boktitler med videre brukes ofte en rettsområdebetegnelse for ¬ vise til en gruppe lover og andre rettskilder som det kan være hensiktsmessig å behandle i en form for systematisk sammenheng. Innen et angitt rettsområde kan man vente å finne felles eller sammenlignbare begreper, partskategorier,

[475] Det litt nedsettende uttrykket «law of the horse» har vært brukt for å kritisere fenomenorienterte betegnelser på rettsområder: «(…) the best way to learn the law applicable to specialized endeavors is to study general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on «The Law of the Horse» is doomed to be shallow and to miss unifying principles.» Frank H. Easterbrook (1996): «Cyberspace and the Law of the Horse». I: *University of Chicago Legal Forum,* s. 207–216.

[476] Et eksempel – som ikke belegges i denne generelle formen, men som henger sammen med noen mer detaljerte senere observasjoner – kan være vektleggingen av pasientautonomi innen helserett. I helserettslig litteratur får kanskje pasientautonomien en høyere status, som et grunnleggende hensyn, enn det ville være dekning for om man ser på helserettslig og personopplysningsrettslig regulering i sammenheng.

gjenstander, handlingstyper og beslektede overordnede hensyn.[477] Rettsområders navn og avgrensning fastlegges ikke i formelle beslutningsprosesser, de blir til gjennom bruken og den tilslutning de får innen et fagfellesskap.[478] En systematisk inndeling gir på ingen måte vanntette garantier for at et bestemt fenomen i samfunnet helt og holdent kan sies å høre inn under et bestemt område. Tvert imot er sammenfall og overlapp mellom etablerte rettsområder svært vanlig, og nærmest uunngåelig.

For å analysere et fenomen i samfunnet som er omfattet av flere rettsområder, kan man velge mellom to prinsipielt forskjellige strategier. Den ene er parallelle analyser, der fenomenet drøftes i lys av hvert av rettsområdene. Den andre strategien er å definere et nytt rettsområde, som integrerer de delene av de «gamle» systematikkene som er relevante for det fenomenet man studerer. Man kan anta at parallelle analyser egner seg best til å løfte frem og synliggjøre motstrid og problemområder av ulike art, mens bygging av en ny systematikk vil peke mer i retning av et harmonisert syn på reguleringen.

I denne avhandlingen er noen sider ved behandlingen av helseopplysninger gjenstand for analyse. Sammenhenger mellom helserettens og personopplysningsrettens begreper og systematikk er sentrale elementer i analysen. Dermed kunne det virke nærliggende å velge strategi nummer to ovenfor, å konstruere «helseopplysningsrett» som et eget rettsområde med disse sammenhengene som emne. Den fristelsen bør likevel motstås i overskuelig fremtid, fordi det er fare for at analysen da ville få et preg av harmoni og avstemthet som ikke yter disse relativt komplekse sammenhengene rettferdighet. En mer pragmatisk grunn til ikke å forsøke å konstruere en egen «helseopplysningsrett» er faren for å bevege seg bort fra både helserettens og personopplysningsrettens kunnskapsmiljøer.[479]

---

[477] Et eksempel fra kapittel 4.3.2 kan illustrere begrepsfelleskap innen et rettsområde: «Aksept av risiko» innen informasjonssikkerhet og lignende internkontrollbasert regelverk betyr en erkjent og dokumentert feiltoleranse som en virksomhet tar på egen kappe, mens en erstatningsrettslig «aksept av risiko» nærmest betyr det motsatte, at en annen person eller virksomhet skal bære risikoen.

[478] Det finnes imidlertid også formaliserte bibliografiske systematikker over rettsområder, som vedlikeholdes av en redaksjon for vedkommende systematikk. For eksempel har Lovdata, Gyldendal Rettsdata og BibJure hver sin hierarkisk ordnede inndeling i rettsområder, som alle er i bruk blant ulike aktører. Felles for disse redaksjonelt besluttede systematikkene er at de fører til høye antall definerte rettsområder. De inneholder koder for atskillig flere områder enn de som normalt brukes i juristers dagligtale eller i oversiktslitteratur. En konstruert bibliografisk systematikk vil antakelig være noe mindre dynamisk enn en uformell tilslutning til å navngi et nytt rettsområde. Mange av de samme betraktningene som man kan gjøre seg om medisinske kodeverk, jf. kapittel 5.1.1.1, vil også være relevante for redaksjonelt besluttede systematikker over rettsområder.

[479] Som et lite apropos til tanken – som altså er forkastet her – om å etablere helseopplysningsrett som en egen disiplin, vises det til en kort drøfting av en lignende begrepsdannelse, helseforskningsrett, i en anmeldelse av boken Sigmund Simonsen og Magne Nylenna (2005): *Helseforskningsrett: den rettslige regulering av medisinsk og helsefaglig forskning*: «Helseforskningsrett er ikke – slik man kan få inntrykk av både gjennom tittelen og ved å lese boken – etablert som egen fagdisiplin innen rettsvitenskapen. Det er derfor heller ikke et innarbeidet begrep blant helserettsjurister, og det er første gang jeg er blitt presentert for det. Hvis det blir vedtatt en lov med særskilt regulering av medisinsk forskning, vil det etter min vurdering være naturlig å definere dette inn under fagdisiplinen 'helserett'.» Bente Ohnstad (2006): «Medisinsk forskning og jus». I: *Tidsskrift for Den norske*

Strategi nummer én ovenfor er valgt i stedet. Den personopplysningsrettslige og den helserettslige reguleringen av behandling av helseopplysninger gjennomgås først og fremst hver for seg. Dernest sammenholdes de delene av reguleringene som har betydning for det å uttrykke, etterleve og følge opp tilgangskriterier, for å vurdere mulig sammenfall, motstrid eller komplementaritet. Grunnantakelsen er at personopplysningsrettens og helserettens regler om behandling av helseopplysninger i de fleste tilfeller vil være komplementære, altså utfylle hverandre, uten at regler fra det ene rettsområdet vanskeliggjør tolkning av regler fra det andre rettsområdet. Det finnes imidlertid noen kandidater til problemer i sammenhengen mellom rettsområdene, eksempelvis i ulike regler om samtykke, forskjeller i hvordan reglene er rettet mot henholdsvis virksomheter og enkeltpersoner, og i at hvert av rettsområdene er gjenstand for tilsyn fra hvert sitt statlige tilsynsorgan.

6.1.2 Europa og verden i norsk regulering av helseopplysninger

Personopplysningsretten og helseretten i Norge er både i ulik grad og på ulike måter knyttet til europeisk og internasjonal regulering og standardisering. Både retten til helsehjelp og retten til vern av privatlivet omfattes av menneskerettskonvensjoner som er gjort gjeldende som norsk lov.[480] Menneskerettene innebærer forpliktelser for staten, som på flere måter kan ha betydning for håndtering av helseopplysninger. For det første skal staten selv ikke gripe inn i privatlivet, terskelen for unntak er høy. Staten skal også beskytte rettighetene mot overtramp fra en tredjepart. For det tredje har staten en plikt til å oppfylle rettighetene, ved å treffe nødvendige regulatoriske og styringsmessige tiltak. Spørsmålene her dreier seg primært om det tredje punktet, de mer strukturelle sidene ved hvordan staten oppfyller rettighetene.

Personopplysningsrettslige regler, i den relativt moderne formen som primært er rettet mot virksomheters elektroniske behandling av opplysninger, ble etablert over få år i mange land, og med bakgrunn i betydelige innslag av internasjonal idéutveksling og normerende anbefalinger.[481] Da EU vedtok sitt personverndirektiv var det i stor grad basert på prinsipper som

---

legeforening, s. 1366–1367. Dette sitatet peker på innarbeidingen i rettsvitenskapelige fagmiljøer som et kriterium for hva som kan anses som et rettsområde.

[480] Den europeiske menneskerettskonvensjon artikkel 8 om respekt for privatliv, FN-konvensjonen om økonomiske, sosiale og kulturelle rettigheter artikkel 12 og barnekonvensjonen artikkel 24 om rett til den høyest oppnåelige helsestandard, jf. menneskerettsloven.

[481] Den amerikanske rapporten *Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens* (1973), OECDs retningslinje *The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) og *Europarådets konvensjon og rekommandasjoner om persondatabeskyttelse* (1981) er blant de anbefalingene som bidro til tidlig harmonisering av ulike lands personopplysningsrettslige reguleringer.

allerede var innarbeidet både i Norge og i flere andre land.[482] Hensikten med direktivet var blant annet å harmonisere beskyttelsesnivået i medlemslandene, for derved å gjøre det mulig å utveksle personopplysninger mellom landene. Personopplysningsloven og helseregisterloven er begge solid forankret i dette direktivet.

Helseretten har, i hvert fall foreløpig, ikke samme direkte tilknytning til EU-regelverk. Relativt lite av helselovgivningen er forankret i EU-direktiver.[483] Annen internasjonal faglig og teknisk standardisering har så langt hatt større innflytelse på norsk helserettslig regulering. Internasjonale kodeverk for sykdommer, funksjon og behandlingsprosedyrer er en form for faglig standardisering, som også har funnet veien inn i detaljreguleringer.[484] Internasjonale profesjonsnettverk har bidratt med viktige premisser i reguleringen, kanskje særlig gjennom krav til informert samtykke som grunnleggende etisk prinsipp i medisinsk forskning.[485] Lovfestede pasientrettigheter, som en tydeliggjort del av helseretten, kan også ses som en del av en internasjonal bevegelse. Det er riktignok sparsomt med henvisninger til påvirkning fra andre land eller fra internasjonale organisasjoner i pasientrettighetslovens tidlige forarbeider og i helserettslig teori.[486] Andre kilder viser elementer av en internasjonal trend som i det minste pågikk samtidig med utviklingen av de norske pasientrettighetene.[487]

Det foregår for tiden en drakamp i EU om et interessant forslag til et nytt pasientrettighets-direktiv.[488] Direktivforslaget er ikke en «enslig svale», det står i en sammenheng med annet regelverk og praksis i EU-domstolen, noe av det omtalt i forslagets fortale. En bred anlagt analyse av direktivforslaget, og omkringliggende regelverk, konkluderer med at det inngår i en mer omfattende europeisk harmonisering av helseretten enn bare det som vanligvis regnes

---

[482] EP/Rdir 95/46/EF.

[483] En viss tiltakende trend er det likevel, blant annet innen legemidler og kontroll med medisinsk utstyr. Et annet eksempel, som så vidt berører randsonen av avhandlingens tema, er autorisasjon av helsepersonell. Der gjelder forskrift om helsepersonell fra EØS-land, 8. oktober 2008 nr. 1130, en forskrift i medhold av helsepersonelloven, som implementerer EP/Rdir 2005/36/EF.

[484] I kapittel 5.1.1.1 er noen slike kodeverk, flere av dem internasjonale, omtalt.

[485] World Medical Association, «Declaration of Helsinki: Ethical Principles for Research Involving Human Subjects»: *http://www.wma.net/en/30publications/10policies/b3/index.html*.

[486] Pasienters rettigheter har primært vært drøftet som en rett til å få helsehjelp, men rettigheter knyttet til behandlingen av helseopplysninger var også en del av den faglige diskusjonen på 1980-tallet og begynnelsen av 1990-tallet. Jf. for eksempel Asbjørn Kjønstad (1982): «Pasienters rettigheter – kontraktsrett eller forvaltnings-rett?». I: *Lov og frihet: festskrift til Johs. Andenæs på 70-årsdagen*, s. 587–602, eller NOU 1992:8.

[487] Det første land som fikk en egen pasientrettighetslov var Finland, med *Lag om patientens ställning och rättigheter*, 17. august 1992 nr. 785. Amsterdamerklæringen om pasientrettigheter ble gitt ut av WHO/EURO, dokumentets formål var å være «a contribution to support the growing interest in many Member States in the issues of patients' rights.» *A Declaration on the Promotion of Patients' Rights in Europe* (1994).

[488] KOM(2008) 414. «Forslag til Europa-parlamentets og rådets direktiv om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser». Stortinget har allerede vedtatt en endringslov, 19. juni 2009 nr. 72 (ikke i kraft ennå), som blant annet innfører en ny § 5-24a i folketrygdloven, som gjennomfører deler av dette direktivforslaget(!)

som pasientrettigheter.[489] Drakampen dreier seg om hvorvidt forslagene til å rettighetsfeste grenseoverskridende helsetjenester i for stor grad overkjører medlemsstatenes rom for å beslutte prioriteringer, og om refusjonsordningene skaper urettferdige markedslignende mekanismer som vanskeliggjør et lands arbeidsmuligheter for å opprettholde en akseptabel standard for alle.[490] For denne avhandlingens del er det imidlertid verken retten til grenseoverskridende helsetjenester eller drakampen som sådan som er interessant. Derimot er det verdt å merke seg at direktivutkastet fastslår, som en klar forutsetning, at vernet av helseopplysninger om pasienten skal ivaretas gjennom personverndirektivet. Den siden ved utkastet til pasientrettighetsdirektiv har ikke vært omstridt. Flere steder i utkastet til pasientrettighetsdirektiv fremgår det at personverndirektivet er en ramme som ikke endres gjennom dette forslaget, og det er heller ikke foreslått noen former for supplerende regulering av behandlingen av helseopplysninger.

> de grundlæggende rettigheder til beskyttelse af privatlivets fred i forbindelse med behandling af personoplysninger respekteres i overensstemmelse med de nationale foranstaltninger til gennemførelse af fællesskabsbestemmelser om beskyttelse af personoplysninger, særlig direktiv 95/46/EF og direktiv 2002/58/EF.[491]

Et annet EU-initiativ, der man finner samme avklaring av at personopplysningsvernet skal ivaretas gjennom det generelle personverndirektivet og ikke i egne helserettslige regler om behandling av opplysninger, er handlingsplanen for e-helse.[492] Med en viss fare for at resonnementet kanskje trekkes litt langt: En europeisering av helseretten kan innebære en utvikling i retning av et skarpere skille mellom personopplysningsrettslige og helserettslige regler om behandling av helseopplysninger. Det kan, i det minste som et teoretisk tankeeksperiment, innebære at de delene av helseretten som dreier seg om å beskytte helseopplysninger beveger seg ut av helseretten, for etter hvert bare å bli ivaretatt gjennom den personopplysningsrettslige reguleringen.

[489] Wolf Sauter (2009): «The Proposed Patients' Rights Directive and the Reform of (Cross-Border) Healthcare in the European Union». I: *Legal issues of economic integration,* s. 109–131.
[490] Forslaget har vært modifisert med kompromissforslag i flere runder, senest 1. desember 2009 ble det blokkert ved at fem medlemsstater stemte mot det modifiserte forslaget.
[491] KOM(2008) 414, artikkel 5(1)(f).
[492] KOM(2004) 356. «E-sundhed – et bedre sundhedsvæsen for Europas borgere: En handlingsplan for et europæisk e-sundhedsområde». Handlingsplanen er knyttet til «Information Society»-aktivitetene i EU.

6.1.3 Spørsmålet om eierskap til helseopplysningene

Reguleringen som omgir helseopplysninger dreier seg om at noen har plikt til å produsere dem, at det gjelder visse krav til hvordan opplysningene skal behandles, og rettigheter for den personen opplysningene gjelder. Verken den helserettslige eller personopplysningsrettslige reguleringen knytter behandling av helseopplysninger til noe konvensjonelt eierbegrep. Likevel forekommer det at ulike syn på rettigheter og plikter begrunnes med en råderett basert på eierskap.

Tidligere har det ikke vært uvanlig å anse sykejournaler som den enkelte leges eiendom.[493] Legen dokumenterte først og fremst for sin egen senere bruk, i tillegg til at dokumentasjonsplikten var nødvendig for faglig tilsyn. Legestanden var lenge skeptiske til å gi pasienter innsyn i sykejournalen, både fordi opplysningene ble ansett som legens eiendom og fordi man regnet med at muligheten for innsyn ville påvirke måten journaler føres på.[494] Et ferskere eksempel er en sak der en lege avviklet et samarbeid med andre leger i et legesenter, hvor spørsmålet var om legen hadde anledning til å ta med seg ut igjen de journalene han hadde brakt med seg inn i legesenteret ti år tidligere. Lagmannsretten brukte ordet «tilhøre» i sin argumentasjon, noe som indikerer at de la et slags eierbegrep til grunn.[495] Da saken senere var oppe i Høyesterett, ble lagmannsrettens bruk av ordet «tilhøre» mildt imøtegått.[496]

Et motstykke til å se helseopplysninger som helsepersonellets eiendom, kunne være å betrakte pasienten som eier. Den helserettslige reguleringen gir ikke helt direkte holdepunkter for en slik betraktning, men det forekommer likevel at pasientens råderett, til tross for at den i mange tilfeller er begrenset, ses som en slags variant av et eierskap. I kommentarutgaven til pasientrettighetsloven bemerkes det at «[d]et er likevel nyttig at det i en pasientrettighetslov understrekes at taushetsbelagte opplysninger kan ses som 'pasientens eiendom'.»[497] De anførselstegnene som kommentarutgavens forfatter har plassert her markerer antakelig at dette forstås mer som en allusjon enn som en direkte analogi.

---

[493] Olaf Trampe Kindt (1957): «Fremleggelse av sykejournaler som bevis i rettssak». I: *Norsk retstidende,* s. 129–135. (s. 130). Artikkelen siterer fra en dom i Hammerfest byrett 21. april 1956: «Journalen var legens eiendom og inneholdt hans private opptegnelser over sykdomstilfellet.»

[494] Slike argumenter er blant annet fremført i de sakkyndiges utførlig refererte uttalelser i sykejournaldommen, Rt. 1977 s. 1035. Høyesteretts resultat er imidlertid ikke basert på noe eierskapsbegrep.

[495] Borgarting lagmannsrett, LB-2006-1155: «Lagmannsretten finner derfor at utgangspunktet må være at en leges skriftlige nedtegninger må tilhøre og forvaltes av ham, med de begrensninger som lovgivningen til enhver tid oppstiller av hensyn til pasienten.»

[496] Rt. 2006 s. 1275, avsnitt 32: «Lagmannsrettens uttalelse om at nedtegnelser « tilhører » og forvaltes av den legen som har skrevet dem, må forstås på bakgrunn av at tvisten er mellom lege og legesenter, og ikke mellom pasient og lege.» Høyesterett kom imidlertid til samme resultat som lagmannsretten, begrunnet med at opplysningene bør følge den som har taushetsplikten.

[497] Aslak Syse (2009): *Pasientrettighetsloven. Med kommentarer*, s. 282. Kommentaren gjelder pasientrettighetsloven § 3-6(2), «Taushetsplikten faller bort i den utstrekning den som har krav på taushet, samtykker.»

I en bred, komparativ analyse av personopplysningsretten er det hevdet at forestillinger om eierrettigheter har spilt en rolle som inspirasjonskilde for lovreguleringen av personopplysningsvern.[498] Prinsipielt kunne både den databehandlingsansvarlige og den registrerte tenkes å ha noe som ligner eierrettigheter. Det å kreve samtykke fra den registrerte som grunnlag for å berettige behandling av opplysninger leder kanskje tankene mest i retning av å skulle se den registrerte som en slags eier. På den annen side vil den databehandlingsansvarlige i mange tilfeller også kunne basere seg på alternative berettigende grunnlag, som i mindre grad involverer den registrerte. De mange unntakene fra den registrertes råderett gjør det vanskelig å trekke konsekvente analogier mellom eierrettigheter og råderettigheter over personopplysninger.

I den rettslige reguleringen av behandling av helseopplysninger er altså begrepet «eier» lite relevant, utover å være en spore til å forstå og tydeliggjøre interessene bak reguleringen. Man støter imidlertid også på forestillinger om eierskap til helseopplysninger i en litt annen sammenheng, ved at det er en godt innarbeidet metafor i en del informatisk teori om tilgangskontroll. Oppfatninger om hvem som «eier» et informasjonselement er ofte noe som representeres i et tilgangskontrollsystem. Ulike eierbegreper er en kilde til store forskjeller mellom de enkelte autorisasjonsprinsippene. Virksomhetsstyrte, sentraliserte modeller for tilgangskontroll bygger på at virksomheten eier opplysningene. Skjønnsbaserte delegeringsmodeller bygger på at den databrukeren som produserer opplysningene er eier.[499] Et tredje perspektiv, som særlig har blitt aktuelt som et teknologisk autorisasjonsprinsipp etter utbredelsen av internett, er å betrakte pasienten eller den registrerte som eier. Innen e-helse og andre nyere anvendelser der den registrerte selv slipper til med større eller mindre direkte adgang til datakildene, har eierbegrepet blitt vendt utover som begrunnelse for at pasienten skal kunne bestemme over tilgangene.

Eierbegreper har visse konnotasjoner, som medfører en fare for at den teknologiske representasjonen av informasjonseierskap vil kunne påvirke hvordan den rettslige reguleringen av behandling av helseopplysninger blir oppfattet. En eventuell slik tilbakeføring fra valget av ordet «eier» som metafor innen tilgangskontroll, til at ulike aktører kan komme til å tolke andre meninger inn i denne metaforen, forfølges imidlertid ikke videre i avhandlingen.

[498] Lee A. Bygrave (2002): *Data protection law: approaching its rationale, logic and limits*, s. 120.
[499] Disse to grunnleggende variantene er omtalt i kapittel 2.3.4 ovenfor.

6.2 Grunnleggende virkemidler i personopplysningsretten

Historie, teoretisk fundament og verdigrunnlag for personopplysningsvern i Norge er godt og grundig beskrevet i flere tidligere arbeider, og denne fremstillingen tar ikke sikte på å bidra med noen nye perspektiver på de bakenforliggende hensynene.[500] Dette er primært en drøfting av personopplysningsrettens virkemidler, med vekt på å undersøke hvilke føringer disse legger for plikten til og metodene for å kontrollere tilgang til og videreformidling av helseopplysninger.

Personopplysningsrettens reelle utgangspunkt er at personopplysninger kan behandles, når det er tilstrekkelig gode grunner til det. Om dette utgangspunktet formuleres som noe i retning av at behandlingen er «tillatt, men bare hvis…» eller «forbudt, med mindre…» kan betraktes som et pragmatisk, fremstillingsteknisk valg.[501] Den som skal behandle personopplysninger må ha en holdbar berettigelse for å gjøre det. Gitt at den holdbare berettigelsen finnes, gjelder ulike bestemmelser om hvordan behandlingen skal foregå.

I fugleperspektiv dreier personopplysningsrettens viktigste regler seg om tilstrekkelig tydelig plassering av ansvar for behandling av opplysninger, hvilke grunnleggende vilkår som gjelder for at behandlingen skal være tillatt, og krav til hvordan opplysningene skal behandles dersom behandlingen i utgangspunktet er tillatt. En måte å dele inn ulike bestanddeler av personopplysningsrettslig regulering, er et knippe overordnede prinsipper som i større eller mindre grad gjenfinnes i en rekke slike regelverk.[502] Det ene av disse prinsippene er rettmessig behandling, som kan ses som synonymt med *vilkår*, som nevnt ovenfor. Andre prinsipper er minimalitet, formålsspesifisering, datakvalitet, den registrertes medbestemmelse og kontroll, begrensninger i adgangen til videreformidling, informasjonssikkerhet, og et prinsipp om sterkere beskyttelse av mer følsomme opplysninger. Disse prinsippene er til dels

[500] Toneangivende fremstillinger er blant annet Knut Selmers innledning i Djønne m. fl. (1987), og Dag Wiese Schartum og Lee A. Bygrave (2004): *Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger*. Jeg har også selv skrevet en liten «dramatisering» (som riktignok ikke hører til blant de toneangivende) om ulike aktørgruppers interesser og perspektiver på helseopplysninger. Herbjørn Andresen (2008b): «Kven skal trøyste Hypomone? Eit kammerspel i tre akter om vern av pasientopplysningar ». I: *Syn og Segn*. Årg. 114, nr. 1, s. 52–61.

[501] Personverndirektivet, EP/Rdir 95/46/EF, ligger nærmest den første fremstillingsformen i sin artikkel 7, som gjelder personopplysninger generelt, og den andre formen i artikkel 8, som gjelder særlige typer opplysninger (herunder helseopplysninger). Personopplysningsloven bruker formuleringen «kan bare behandles dersom …» i begge tilfeller, altså både i §§ 8 og 9.

[502] Den korte oversikten som følger er basert på kapitlet «Core Principles of Data Protection Laws», i Bygrave (2002), s. 57 ff.

nedfelt i personopplysningsloven som «grunnkrav», og til dels fordelt over andre bestemmelser i loven.[503]

Helseregisterloven er i hovedsak det personopplysningsrettslige hjemmelsgrunnlaget for behandlingen av helseopplysninger. Personopplysningsloven kommer inn i bildet på to måter, delvis ved at behandlingen av helseopplysninger i visse situasjoner faller utenfor helseregisterlovens virkeområde, og delvis ved at den gjelder som utfyllende bestemmelser til helseregisterloven. Det er først og fremst denne norske implementasjon av personverndirektivet som er gjenstand for drøfting, men i enkelte situasjoner er det også behov for å trekke inn direktivets tekst. En type situasjon der det kan være mest hensiktsmessig å vurdere noe direkte opp mot personverndirektivet er når resonnementer er lånt inn fra internasjonale teoretiske bidrag. Ellers må henvisninger til «Artikkel 29-gruppen» og deres mandat nødvendigvis ta utgangspunkt i direktivet. Artikkel 29-gruppen er en arbeidsgruppe som dekker hele direktivets nedslagsfelt, og kan derfor ikke gjenfinnes i noen parallell bestemmelse i norsk lovgivning. Gruppen har sitt navn fra direktivets artikkel 29, og har til oppgave å følge opp personverndirektivet og koordinere arbeidet mellom landene. Artikkel 29-gruppen produserer både rettspolitiske «opinions» og vurderinger av medlemsstaters og tredjelands beskyttelsesnivå. Arbeidsgruppens autoritet fra direktivet, og det at de ser personopplysningsvernet i hele EU/EØS-området i sammenheng, gir grunnlag for å tillegge deres uttalelser betydelig vekt.

6.2.1 Ansvarsplassering etter personopplysningsretten

Et viktig element i personopplysningsretten er spørsmålet om hvor ansvaret og pliktene skal plasseres. Utgangspunktet er et legaldefinert begrep, som styrer plasseringen. Helseregisterloven definerer en rolle som databehandlingsansvarlig, som er «den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes, hvis ikke databehandlingsansvaret er særskilt angitt i loven eller i forskrift i medhold av loven.»[504] Setningsleddet *hvis ikke…* kan nærmest leses som en oppfordring til å avklare databehandlingsansvaret direkte i lov eller forskrift. Den funksjonen som helseregisterloven kaller databehandlingsansvarlig, kalles i personopplysningsloven behandlingsansvarlig.[505] Legaldefinisjonen av behandlingsansvarlig er noe kortere, den har ikke med det som kommer etter

[503] Personopplysningsloven § 11 har overskriften «Grunnkrav til behandling av personopplysninger». Det grunnkravet som først og fremst er vektlagt i denne avhandlingen er prinsippet om begrensninger i adgangen til videreformidling, som i personopplysningsloven § 11 er tett sammenfiltret med prinsippet om formålsspesifisering. Formålsspesifisering, formålets betydning for adgangen til videreformidling, er også sentrale elementer i tilsvarende bestemmelser både i helseregisterloven § 11 og i personverndirektivet artikkel 6.
[504] Helseregisterloven § 2(1)(8).
[505] Personopplysningsloven § 2(1)(4).

komma i helseregisterlovens definisjon. Behandlingsansvar etter personopplysningsloven kan også angis direkte i lov eller forskrift, selv om denne muligheten ikke nevnes i definisjonen.[506] Valget som er gjort i helseregisterloven, om å kalle denne rollen databehandlingsansvarlig i stedet for behandlingsansvarlig, er ikke ment som en endring av meningsinnholdet. Det er kun gjort for å unngå sammenblanding med ansvaret for å behandle pasienter i form av å yte helsehjelp.[507]

I proposisjonen til personopplysningsloven ble det presisert at bare subjekter som har partsevne kan være behandlingsansvarlig.[508] Dette kriteriet er det resonnert litt videre rundt i et rundskriv som gjelder enkelte bestemmelser i helseregisterloven og helsepersonelloven som har betydning for hvordan opplysninger fra pasientjournaler kan utleveres.

> Den databehandlingsansvarlige pålegges en rekke plikter i helseregisterloven. Helseregisterloven § 16 stiller blant annet krav om at databehandlingsansvarlig i forhold til utenverden skal stå inne for at informasjonssikkerheten er tilfredsstillende, slik at konfidensialitet, integritet, kvalitet og tilgjengelighet blir godt nok ivaretatt. Blant annet fordi manglende oppfyllelse av denne plikten er straffesanksjonert og fordi den registrerte skal kunne få håndhevet sine rettigheter etter loven, er det et krav at databehandlingsansvarlig må ha partsevne – det vil si kunne saksøkes for domstolene. Dette innebærer også at delegasjon av databehandlingsansvaret til enheter som ikke har partsevne, bare vil omfatte det daglige ansvaret for behandlingen av opplysningene.[509]

Både helseregisterloven og personopplysningsloven har gitt definisjonen en form som tyder på at ansvaret fortrinnsvis bør være entydig plassert, altså i én enkelt virksomhet. Personverndirektivet stiller dette helt eksplisitt mer åpent, i sin definisjon av behandlingsansvarlig: «den fysiske eller juridiske person … som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal benyttes.»[510] I proposisjonen til personopplysningsloven erkjente departementet muligheten av at en og samme behandling kan ha flere ansvarlige, slik direktivet også åpner for, men bemerket at man bør tilstrebe å plassere behandlingsansvaret i ett og samme organ.[511]

---

[506] Et eksempel er Helfos saksbehandling av refusjonskrav, der folketrygdloven § 21‑11a (6) utpeker Helsedirektoratet som behandlingsansvarlig etter personopplysningsloven.
[507] «… for på den måten å få frem forskjellen mellom behandling av enkeltpasienter og behandling av helseopplysninger», Ot.prp. nr. 5 (1999-2000), s. 5.
[508] Ot.prp. nr. 92 (1998-1999), s. 103.
[509] *Rundskriv vedrørende tilgang til og utlevering av opplysninger i elektroniske pasientjournaler.* (2006), s. 5.
[510] EP/Rdir 95/46/EF artikkel 2(1)(d). Ulike modeller for samhandling der flere er ansvarlig for samme behandling er drøftet blant annet i Thomas Olsen og Tobias Mahler (2007): «Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II». I: *Computer Law & Security Report,* s. 415–426.
[511] Ot.prp. nr. 92 (1998-1999), s. 103.

Utover det som fremgår av helseregisterlovens definisjon, er hovedregelen for plassering av databehandlingsansvar i *behandlingsrettede* helseregistre at den virksomheten som tar registeret i bruk er databehandlingsansvarlig for opplysningene.[512] For helseregistre som har større nedslagsfelt enn å være et virksomhetsinternt register er det svært utbredt å fastlegge i lov eller forskrift hvem som skal være databehandlingsansvarlig, og dermed også plassere dette ansvaret hos ett organ.[513]

Det ansvar og de plikter som drøftes i denne avhandlingen kan belyses i tilstrekkelige grad med bare å henvise til den databehandlingsansvarlige. Det er likevel også verdt å nevne *databehandler*, som er en annen rolle som er definert både i helseregisterloven og i personopplysningsloven.[514] En databehandler kan i realiteten utføre alt praktisk og teknisk arbeid med behandlingen av opplysninger, men de har ingen egen råderett over opplysningene og kan bare behandle dem i henhold til avtale med databehandlingsansvarlig. Reguleringen av forholdet mellom databehandlingsansvarlig og databehandler dreier seg om å holde fast det endelige ansvaret hos den databehandlingsansvarlige i vertikale oppdragsforhold.

6.2.2 Ulike typer opplysninger og forskjeller i beskyttelsesbehov

6.2.2.1 Forskjeller i hvor presist en person er identifisert

For at en opplysning i det hele tatt skal være en personopplysning, må den kunne knyttes til en enkeltperson. Det samme kriteriet gjelder for at noe skal være en helseopplysning, i tillegg til at det da må gjelde taushetsbelagte opplysninger i henhold til helsepersonelloven § 21, eller andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold.[515] Prinsipielt sett skal den som behandler personopplysninger avstå fra å identifisere enkeltpersonen mer presist enn det er behov for. Personopplysningslovens bestemmelser om bruk av fødselsnummer peker på et slikt prinsipp, selv om dette ikke fungerer særlig effektivt som begrensning i praksis.[516]

---

[512] Helseregisterloven § 6(2).

[513] Konkret plassering av databehandlingsansvar er gjennomført i alle forskrifter om sentrale helseregistre etter helseregisterloven § 8. De generelle bestemmelsene om adgang til å etablere virksomhetsovergripende behandlingsrettede helseregistre, §§ 6a og 6b, foreskriver også at plasseringen av databehandlingsansvar skal sikres gjennom forskrift.

[514] Jf. personopplysningsloven § 15 og helseregisterloven § 18. Rollen som databehandler, som er en virksomhet som oppgaver er «outsourcet» til, er også omtalt ovenfor i kapittel 4.3.1.1 og 4.5.3.

[515] Jf. definisjonene i personopplysningsloven § 2(1)(1) og i helseregisterloven § 2(1)(1). I personverndirektivet, 95/46/EF artikkel 2(1)(a) omtaler definisjonen «identifisert eller identifiserbar person».

[516] Personopplysningsloven § 12. Det skal være «saklig behov» for sikker identifisering, altså en mindre streng relevansnorm enn å kreve at det må være nødvendig. Bruk av fødselsnummer kan til og med pålegges, dersom det trengs for å sikre opplysningenes kvalitet.

Dersom personopplysningene behandles på en slik måte at det er mindre sannsynlig at enkeltpersoner kan identifiseres, kan det tilsi at man i en samlet vurdering finner at det reduserer behovet for sterke beskyttelsestiltak. Personopplysningsloven inneholder imidlertid relativt få bestemmelser som kan antyde noen sammenheng mellom grad av identifisering og opplysningenes beskyttelsesbehov.[517] I helseregisterloven er det derimot en mer eksplisitt og systematisk sammenheng mellom grad av identifisering og lempelighet både i vilkårene for behandling og i kravene til beskyttelse. Kravene er strengest for å behandle helseopplysninger dersom de er knyttet til personidentifiserende kjennetegn. Både krav til grunnlag for behandlingen og føringer for hva opplysningene kan brukes til er mindre strenge for pseudonyme eller avidentifiserte helseopplysninger.[518] Pseudonymisering, ved at en tredjepart sitter med nøkkelen til å koble et pseudonym til den registrertes reelle identifikator, er kanskje den organisatorisk og teknologisk mest interessante varianten. Det var et radikalt og teknologisk avansert forslag som ble lansert i en offentlig utredning allerede i 1993.[519] Muligheten for å etablere pseudonyme helseregistre kom inn i lovgivningen med helseregisterloven i 2001, men selv om dette er et alternativ som åpner for mer bruk av opplysningene i et register, har det likevel fått en noe kjølig mottakelse hos sentrale myndigheter med behov for å behandle helseopplysninger og i de epidemiologiske forskningsmiljøene.[520] Både pseudonyme og avidentifiserte helseregistre finnes i dag, men bare i svært beskjedent antall.[521] Bruk av fødselsnummer er den dominerende identifikasjonsmåten for helseopplysninger de aller fleste steder og i de aller fleste situasjoner.

[517] Relevanskriterier for bruk av fødselsnummer kan i seg selv sies å indikere en slik sammenheng. En annen bestemmelse som peker på sammenhengen er personopplysningsloven § 28: Lagring av personopplysninger for historie og statistikk kan overstige lagringstiden som følger av det opprinnelige formålet, dersom samfunnets interesse i lagringen overstiger ulempene for den enkelte. «Den behandlingsansvarlige skal i så fall sørge for at opplysningene ikke oppbevares på måter som gjør det mulig å identifisere den registrerte lenger enn nødvendig», § 28(2)(2).

[518] Pseudonyme og avidentifiserte helseopplysninger har egne definisjoner i helseregisterloven § 2(1), henholdsvis nr. (4) og (2). Opplegget for mindre strenge vilkår og krav følger primært av §§ 7 og 8.

[519] NOU 1993:22.

[520] En mer detaljerte redegjørelse for dette finnes i Herbjørn Andresen (2009): «The Policy Debate on Pseudonymous Health Registers in Norway». I: *Biomedical Engineering Systems and Technologies*, s. 413–424.

[521] Det er etablert to sentrale pseudonyme registre, Reseptregisteret og Individbasert pleie- og omsorgsstatistikk (IPLOS). Det finnes tre sentrale avidentifiserte registre, Abortregisteret, Norsk overvåkingssystem for infeksjoner i sykehustjenesten (NOIS), og Norsk overvåkingssystem for antibiotikaresistens hos mikrober (NORM). I tillegg finnes det en del situasjoner der helseopplysninger bare kan utleveres i avidentifisert form, selv om registeret som sådan er personidentifiserbart. Norsk pasientregister (NPR) ble opprinnelig etablert som et avidentifisert register i 1997, men har blitt omgjort til et personidentifiserbart register i medhold av endringslov 16. februar 2007 nr. 7.

6.2.2.2 Særlige typer opplysninger, og grader av sensitivitet

Et av personopplysningsrettens sentrale begreper er vilkår, eller kriterier, for at behandling av personopplysninger skal være lovlig.[522] Vilkårene er inndelt i to nivåer, det ene er de som gjelder for personopplysninger generelt, det andre nivået er skjerpede vilkår, eller kriterier, for behandling av bestemte typer opplysninger. I personverndirektivet er dette kalt *særlige typer opplysninger*, med en kort liste over hva slags opplysninger dette er.[523] Personopplysningsloven bruker betegnelsen *sensitive opplysninger* for å dekke samme funksjon, altså for å angi skjerpede vilkår for at behandlingen skal være lovlig.[524] Både etter personverndirektivet og personopplysningsloven er helseopplysninger blant disse særlige typene opplysninger.[525]

Ordet sensitivt betyr følsomt, og har i utgangspunktet vært oppfattet som en subjektiv egenskap. I en gjennomgang av den historiske bakgrunnen for begrepet sensitive opplysninger, beskrives en utvikling fra den subjektivt orienterte betydningen over mot en mer objektivt orientert angivelse av visse typer opplysninger som sensitive.[526] Et objektivt sensitivitetsbegrep bidrar med regulatorisk tydelighet, og til å sikre et nivå av felles standarder som er uavhengig av om den registrerte engasjerer seg i informasjonsbehandlingen. Et subjektivt sensitivitetsbegrep motiverer en større grad av medbestemmelse fra den registrerte. Sensitivitet som et subjektivt eller objektivt begrep er komplementære perspektiver. Det er behov for begge perspektivene, både regulatorisk tydelighet og erkjennelse av at sensitivitet er avhengig av kontekst, selv om det fører til at sensitivitet blir et noe motsetningsfylt begrep.[527]

---

[522] Overskriften til personopplysningsloven § 8 bruker ordet vilkår, mens overskriften til personverndirektivet artikkel 7 kaller det kriterier. Til tross for små nyanseforskjeller fyller disse bestemmelsene samme funksjon i systematikken. Vilkårene som sådan er nærmere drøftet nedenfor i kapittel 6.2.3.

[523] EP/Rdir 95/46/EF artikkel 8(1), definerer dette som «personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religiøs eller filosofisk overbevisning, fagforeningsmedlemskap samt behandling av opplysninger om helse og seksualliv.»

[524] Sensitive personopplysninger er legaldefinert i personopplysningsloven § 2(1)(8), de skjerpede vilkårene er angitt i § 9. I Dag Wiese Schartum og Lee A. Bygrave (2006): «Utredning av behov for endringer i personopplysningsloven: skrevet etter oppdrag fra Justisdepartementet og Moderniseringsdepartementet», s. 15 og 16, anbefales en presisering av denne definisjonen til å gjelde opplysnings*typer*.

[525] Helseopplysninger har alltid vært en opplagt kandidat til skjerpede krav, som man for eksempel kan se av dette sitatet: «Vi vet ikke nøyaktig hva det betyr at en opplysning er sensitiv, men det er enighet om at hvis man kan snakke om 'sensitivitet' i forbindelse med informasjon, så vil helseopplysninger i høy grad ha denne egenskapen.» Knut S. Selmer (1977): «Medisinske informasjonssystemer – en utfordrende blanding av velsignelser og farer». I: *Data og personvern*, s. 117–132. (s. 120).

[526] «Therefore, confidentiality of 'personal data' is justified not principally in the nature of the data itself, but in the nature of the relationship in which they are disclosed or communicated.» Jon Bing (2008): «Notions of sensitive personal data». I: *Défis du droit à la protection à la vie privée/Challenges of Privacy and Data Protection Law*, s. 191–208. (s. 196).

[527] Det motsetningsfylte i dette er også påpekt i Bygrave (2002), s. 69: «Singling out relatively fixed sub-sets of personal data for special protection breaks with the otherwise common assumption in data protection discourse that the sensitivity of data is essentially context-dependant.»

Legaldefinisjonen av *sensitive personopplysninger* knytter sensitivitet til bestemte typer opplysninger. Definisjonen fungerer som en utløsermekanisme for de skjerpede vilkårene for at behandling av opplysningene skal være tillatt. Uttrykket sensitive personopplysninger har i den sammenheng samme meningsinnhold som *særlige typer opplysninger*. I denne avgrensede delen av personverndirektivets og personopplysningslovens systematikk er sensitive versus ikke-sensitive personopplysninger en dikotomi, uten graderinger eller mellomposisjoner. Dette er imidlertid ikke hele bildet. Etter at man har fastslått at det er adgang til å behandle opplysningene, er det andre bestemmelser i personopplysningsloven, og tilsvarende i personverndirektivet og i helseregisterloven, som regulerer hvordan behandlingen skal foregå, og hvilke plikter og rettigheter som gjelder. For de ulike bestemmelsene om hvordan opplysningene skal behandles, finnes det flere innslag av graderinger mellom mer og mindre sensitive opplysninger. Et graderbart sensitivitetsbegrep ligger antakelig nærmere dagligtalebetydningen av ordet sensitivt enn å bruke det som merkelapp på noen bestemte typer opplysninger. Derfor kan det virke noe uheldig at personopplysningsloven, gjennom en skarp definisjon, til en viss grad hekter begrepet «sensitivt» fast i en dikotomi som er styrende for en relativt begrenset del av lovens bestemmelser.

Et område der en henvisning til ulike grader av sensitivitet er nedfelt i reguleringen, finner man i personopplysningsforskriftens kapittel om informasjonssikkerhet.[528] Virksomhetens kontroll med informasjonssikkerheten skal bygge på vurderinger av beskyttelsesbehovet som er mer nyanserte enn dikotomien sensitiv eller ikke-sensitiv. Formuleringene som brukes i forskriften er «personopplysninger hvor konfidensialitet er nødvendig», «personopplysninger hvor tilgjengelighet er nødvendig», og «personopplysninger hvor integritet er nødvendig».[529]

Helseregisterloven definerer ikke i seg selv noen opplysninger som sensitive, noe som er naturlig ettersom hele lovens virkeområde kommer inn under begrepet «sensitivt» slik det er definert i den generelle personopplysningsloven. Likevel har også helseregisterloven ulike krav til hvordan behandlingen skal foregå, og hvilke plikter og rettigheter som gjelder, som varierer med ulike graderinger av følsomhet og beskyttelsesbehov.[530]

---

[528] Personopplysningsforskriften kapittel 2. Dette er et krav til risikobasert internkontroll for informasjonssikkerhet i virksomheter som behandler personopplysninger, og gjelder som utfyllende bestemmelser både til personopplysningsloven § 13 og til helseregisterloven § 16.

[529] *Personopplysningsforskriften,* henholdsvis §§ 2-11, 2-12 og 2-13.

[530] Et eksempel er forutsetningen om at virksomhetsovergripende, behandlingsrettede helseregistre skal bestå av en begrenset mengde opplysningstyper, og ikke skal kunne erstatte den virksomhetsinterne journalen, jf. helseregisterloven § 6a. Et annet eksempel, som gjelder den registrertes rettigheter, er at man kan kreve slettet eller sperret opplysninger som «føles sterkt belastende for den registrerte», altså uavhengig av om opplysningene er riktige eller gale, jf. § 28(1).

Artikkel 29-gruppen peker også på behovet for graderte beskyttelsesmekanismer for ulike grader av sensitivitet, i sin anbefaling om hvordan medlemsland bør regulere den registrertes medvirkningsmuligheter i pasientjournalsystemer.

> In the legal provisions introducing an EHR system, it should be laid down as a rule that entering data into an EHR or accessing such data should be governed by an incremental system of «opt-in» requirements (especially when processing data, which are potentially extra harmful such as psychiatric data, data about abortion, etc.) and «opt-out» possibilities for less intrusive data.[531]

Hele den reguleringen de her anbefaler vil ligge innenfor personverndirektivets artikkel 8, kriterier for å behandle særlige typer opplysninger. Innenfor denne kategorien opererer Artikkel 29-gruppen med en glideskala mellom *potentially extra harmful* og *less intrusive*. Ut fra variasjoner i opplysningenes sensitivitet eller skadepotensial, anbefales det å etablere graderte opplegg for både uttrykkelig samtykke og reservasjonsadgang.

I personopplysningsrettslig regulering har man ikke hatt samme tradisjon som innen militærvesen og institusjoner som arbeider med samfunnssikkerhet for å merke dokumenter eller opplysninger med en sensitivitetsgrad.[532] En del modeller for å uttrykke tilgangskriterier er imidlertid basert på at man i en eller annen form merker hvilke opplysninger som har et angitt beskyttelsesbehov. For eksempel innfører en europeisk teknisk standard for elektronisk kommunikasjon av helseopplysninger en referansemodell for klassifisering av tilgangskriterier, der opplysningstyper skal merkes med en bokstav, mellom A og G, der bokstaven indikerer hvor tunge restriksjoner som legges for videreformidling.[533] En avmerking av et besluttet beskyttelsesbehov vil ikke inngå i alle slags modeller for tilgangskriterier, det vil være mindre behov for en slik avmerkning dersom tilgangskriteriene er basert på dynamiske forløp i behandlingsprosessen i stedet for statiske egenskaper ved opplysningene. Det er heller ikke nødvendigvis slik at hver enkelt opplysning i den enkelte pasientjournal trenger merking, for eksempel kan ulike strukturelementer i en kildeorientert journal merkes sjablongmessig med et generelt antatt beskyttelsesbehov.[534]

---

[531] *Working Document on the processing of personal data relating to health in electronic health records (EHR).* (2007), s. 14.

[532] Jf. den hierarkiske inndelingen i sikkerhetsloven, 20. mars 1998 nr. 10 § 11(1): Strengt hemmelig – hemmelig – konfidensielt – begrenset. Kravet til å merke skjermingsverdig informasjon følger av annet ledd.

[533] ICO/CEN EN 13606 (2007): «Health informatics – Electronic health record communication». Part 4: Security. Modellen er lagt slik opp at mulige mottakere av en opplysning knyttes til hvilken rolle vedkommende har overfor pasienten. Standarden angir imidlertid ikke konkret hvilke opplysninger, eller typer opplysninger, som det for eksempel skal betraktes som gangbart å gjøre tilgjengelig for administrativt personale (bokstav C), og hvilke som bare skal kunne kommuniseres til de som er direkte involvert i behandlingen (bokstav E).

[534] Kildeorientert strukturering av pasientjournal er nærmere beskrevet ovenfor, i kapittel 5.1.1.2.

Selv om personopplysningsrettslig regulering av informasjonssikkerhet ikke stiller spesifikke krav til å merke opplysninger med hvilket beskyttelsesbehov som skal gjelde for dem, vil en del måter å uttrykke tilgangskriterier på innebære et indirekte krav om å angi ulike graderte beskyttelsesbehov. En side ved denne typen indirekte krav er spørsmålet om hvorvidt en virksomhet som behandler helseopplysninger må forhåndsvurdere opplysninger for å ta stilling til om de kan gjøres tilgjengelige for mottakerinitiert overføring til annen virksomhet.[535] En slik forhåndsvurdering vil også kunne bestå av å velge mellom ulike grader av sensitivitet som opplysningene skal merkes med, slik at for eksempel bruk i et virksomhetsovergripende behandlingsrettet register gis en annen terskel enn når man lar helsepersonell fra den mottakende virksomheten få lesetilgang i den avgivende virksomhets informasjonssystem.

6.2.3 Vilkår for og grunnkrav til behandling av opplysninger

Vilkår for og grunnkrav til behandling av personopplysninger, herunder behandling av helseopplysninger, er en vesentlig komponent i den personopplysningsrettslige reguleringen. Det er særlig to grunner til å drøfte denne siden ved reguleringen på et relativt teoretisk plan. Den ene grunnen er at horisontal videreformidling av helseopplysninger på tvers av organisatoriske grenser innebærer at det vil kunne være vekslende grunnlag for behandling i de ulike virksomhetene opplysningene befinner seg i. Den andre grunnen er en forskjell – som i hvert fall tilsynelatende er ganske stor – på samtykke som et av flere mulige vilkår for å behandle helseopplysninger etter personopplysningsretten, og samtykke som et virkemiddel for pasientautonomi og medbestemmelse i helseretten.

Vilkår som berettiger behandling av personopplysninger generelt følger av personopplysningsloven § 8, mens vilkår for å behandle sensitive personopplysninger følger av § 9.[536] Det kreves også konsesjon fra Datatilsynet for å behandle sensitive personopplysninger, riktignok med et relativt omfattende unntak for behandling av personopplysninger i organ for stat eller kommune når behandlingen har hjemmel i lov.[537] Konsesjonsplikten, i de tilfellene der det ikke er gjort unntak fra den, er formelt og systematisk sett en del av det som skal til for å

[535] Behovet for å forhåndsvurdere hvilke opplysninger som kan kommuniseres under hvilke betingelser er en indirekte følge av endringen i helsepersonelloven § 45, lovvedtak 19. juni 2009 nr. 68, der mottakeren gis rett til å motta opplysninger fra virksomheten, til forskjell fra den tidligere innretningen der avgiveren, den som hadde dokumentasjonsplikten, måtte vurdere utleveringen. Spørsmålet om forhåndsvurdering er drøftet i forarbeidene, særlig i Ot.prp. nr. 51 (2008-2009), s. 35.
[536] Jf. definisjonen av sensitive personopplysninger i personopplysningsloven § 2(1)(4), og drøftingen i kapittel 6.2.2.2 ovenfor.
[537] Personopplysningsloven § 33.

berettige behandling av personopplysninger. Datatilsynets prinsipielt åpne mulighet til å sette vilkår for en konsesjon kan i konkrete tilfeller innebære en skjerping av de faste vilkårene som berettiger behandling. Slike konsesjonsvilkår er imidlertid ekstraordinære, og vil ligge noe på utsiden av den generelle systematikken for å berettige behandling av personopplysninger.[538]

Behandling av helseopplysninger etter helseregisterloven forutsetter som et utgangspunkt at vilkårene i personopplysningsloven er oppfylt. Helseregisterloven § 5 henviser til personopplysningsloven §§ 9 og 33, eller alternativt helseforskningsloven, som nødvendige vilkår. Ettersom helseopplysninger i seg selv anses som sensitive, kan ikke personopplysningsloven § 8 gi selvstendig berettigelse for behandling etter helseregisterloven. Kriteriene i personopplysningsloven § 8 er likevel innbefattet, fordi vilkårene i personopplysningsloven § 9 forutsetter at et av vilkårene i § 8 er oppfylt.[539] Det alternative behandlingsgrunnlaget i helseforskningsloven, som helseregisterloven § 5 viser til, er forskningsprosjekter med forhåndsgodkjenning fra den regionale komiteen for medisinsk og helsefaglig forskningsetikk.[540]

Personopplysningsloven §§ 8 og 9 er utgangspunktet for denne drøftingen av vilkår for behandling av personopplysninger. Enkelte perspektiver og argumenter er imidlertid hentet fra teori som drøfter personverndirektivet, det vil derfor noen steder være referert til de tilsvarende bestemmelsene i direktivet.

6.2.3.1 Skillet mellom berettigelse og garantier

Personopplysningsretten bygger på et gjennomgående skille mellom regler som gjelder betingelsene for at behandling av opplysninger skal være lovlig, og regler som gjelder tiltak for å beskytte den registrertes rettigheter forutsatt at behandlingen er lovlig i utgangspunktet. Dette skillet er tydelig både i personopplysningslovens og i personverndirektivets struktur. I

[538] Et eksempel som illustrerer at konsesjonsvilkår kan forstås som en litt annerledes innretning enn de generelle vilkårene i loven, finner man i forarbeid til helseforskningsloven, utredningen NOU 2005:1, s. 94: «Datatilsynet kan i henhold til personopplysningsloven § 35 stille vilkår for at konsesjon skal bli gitt. I praksis vil det kunne oppstå en forhandlingslignende situasjon, der Datatilsynet og konsesjonssøker prøver å finne frem til ordninger som kan forene motstridende interesser og på den måten unngå at søknaden avslås.»

[539] Denne innretningen er litt forskjellig fra personverndirektivet, EP/Rdir 95/46/EF, som ikke har en slik kobling mellom kriteriene for behandling av personopplysninger generelt i artikkel 7 og for behandling av særlige typer opplysninger i artikkel 8.

[540] Jf. helseforskningsloven § 33(1), som fastslår at dette er nødvendig og tilstrekkelig behandlingsgrunnlag for helseopplysninger i medisinsk og helsefaglig forskning.

helseregisterloven fremtrer ikke dette skillet like klart, men det følger av situasjoner der personopplysningsloven har betydningen som utfyllende bestemmelser.[541]

En berettigelse for å behandle helseopplysninger ligger primært i at vilkårene for behandling er oppfylt. Enkelte av grunnkravene dreier seg om å hindre at opplysningene tas i bruk på måter som er i strid med vilkårene, og kan dermed også systematisk sett ses i sammenheng med berettigelsen. Uttrykket «nødvendige garantier» brukes flere steder i personverndirektivet, i den engelske versjonen er uttrykket «appropriate safeguards», som også kunne ha vært oversatt til egnede eller tjenlige beskyttelsestiltak. Nødvendige garantier signaliserer en plikt for medlemslandene til å introdusere rettigheter eller konkrete tiltak for å motvirke ulempene for den registrertes personopplysningsvern. En vesentlig, prinsipiell forskjell mellom berettigelse og garantier er at berettigelse må være på plass før behandlingen av opplysninger kan begynne, mens garantiene får effekt på alle senere trinn under og etter behandlingen. Den registrerte har visse rettigheter, slik som en rett til innsyn i opplysninger om seg selv, rett til å korrigere ukorrekte opplysninger, og i noen situasjoner også til å motsette seg at opplysningene behandles.

Dette strukturelle skillet mellom berettigelse og garantier er gammelt i personopplysningsrettslig teori. En amerikansk offentlig rapport tilrådde i 1973 at de sterke hensynene for å etablere sentrale personregistre måtte balanseres med tiltak – *safeguards for privacy* – både i form av plikter for registervirksomheten og i form av den registrertes rett til innsyn og korrigering. Rapporten fremhevet behovet for tiltak som etablerer en viss grad av gjensidighet, som skulle demme opp for de personvernproblemene registreringen medfører uten å avskjære mulighetene for å etablere og bruke registre.[542] Et tilsvarende skille finner man i OECDs retningslinje fra 1980. Et av prinsippene går ut på at det skal være grunnlag for innsamling av opplysninger, «such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject», og et annet prinsipp går ut på at formålet skal være fastlagt før behandlingen starter.[543] De øvrige prinsippene i retningslinjen gjelder ulike garantier eller tiltak under og etter behandlingen. Denne grunnleggende innretningen av personopplysningsretten har også sine kritikere, blant annet er det

[541] Det gjelder både de konkrete henvisningene til personopplysningsloven, særlig i helseregisterloven §§ 5, 12 og 14, og den generelle bestemmelsen om personopplysningsloven med forskrifter som utfyllende bestemmelser i helseregisterloven § 36.
[542] *The HEW Report*, særlig kapittel III. «Safeguards for personal privacy based on our concept of mutuality in record-keeping would require adherence by record-keeping organizations to certain fundamental principles of fair information practice.»
[543] *The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, s. 14 og 15.

hevdet at gjensidigheten blir illusorisk når vurderinger og operasjonalisering i så stor grad er overlatt til de virksomhetene som behandler opplysningene.[544]

En annen forskjell mellom berettigelse og garantier er spørsmålet om hvilke aktører som er relevante interessenter eller rettighetssubjekter. Enhver, uavhengig av om vedkommende selv er registrert eller ikke, har rett til generell informasjon om behandlingen av opplysninger. Det omfatter informasjon om hvem som er databehandlingsansvarlig, hva som er formålet med behandlingen, hvilke typer opplysninger som behandles, og hvilke kategorier av personer opplysningene gjelder.[545] Personverndirektivet pålegger medlemsstater å publisere et register med generell informasjon om behandlinger, som skal være offentlig tilgjengelig.[546] Dette ivaretas i noen grad ved at Datatilsynet er pålagt å føre en systematisk og offentlig fortegnelse over behandlinger som er meldt inn.[547] Den generelle berettigelsen for behandling av personsopplysninger er således et allment anliggende, underlagt et offentlighetsprinsipp. For garantier og tiltak som beskytter den registrerte, eller gir den registrerte mulighet til å utøve medbestemmelse og kontroll under og etter behandling, er derimot den enkelte registrerte rettighetssubjekt.

6.2.3.2 Berettigelse av prosessuell eller materiell art

Personopplysningsloven §§ 8 og 9 angir ulike kriterier som kan berettige behandling av personopplysninger. Innen hver av disse paragrafene står det et *eller* mellom kriteriene, det er altså tilstrekkelig at ett av kriteriene er oppfylt. Det første kriteriet som er oppført, både i § 8 og i § 9, er at den registrerte har samtykket. Et samtykke kan kalles prosessuell berettigelse, mens de øvrige kriteriene gir en materiell berettigelse. Selv om terskelen for et materielt samtykke kan settes høyt, vil den databehandlingsansvarlige ikke være avhengig av at den registrerte på forhånd har sagt seg enig for å ta stilling til om behandlingen er berettiget.

Prosessuell berettigelse avhenger derimot av hver enkelt registrert persons tilslutning. Berettigelsen finnes ikke a priori, og den kan ikke påregnes.[548] Når samtykke er det vilkåret

[544] Et eksempel på en slik kritikk finnes i Fred H. Cate (2006): «The failure of fair information practice principles». I: *Consumer Protection in the Age of the Information Economy*, s. 341–377, som argumenterer bredt mot den rådende tilnærmingen, og i stedet anbefaler et opplegg med større innslag av rettighetsbasert og forbrukervernlignende regulering.
[545] Personopplysningsloven § 18.
[546] EP/Rdir 95/46/EF artikkel 21(2).
[547] Helseregisterloven § 31(1) jf. personopplysningsloven § 42(3)(1).
[548] Dette er sammenlignbart med betraktningen om prosessuell rettferdighet, som omtalt med henvisning til Rawls (1999) i kapittel 4.5.2 ovenfor, «… the procedure for determining the just result must actually be carried out.»

den databehandlingsansvarlige baserer behandlingen på, må vedkommende både forvente og faktisk akseptere at «nei» kan være svaret på forespørselen om samtykke.

De øvrige vilkårene i personopplysningsloven §§ 8 og 9 vil, dersom de er holdbare, gi en materiell berettigelse. Den klareste formen for materiell berettigelse er at det er fastsatt i lov at det er adgang til slik behandling.[549] En tallmessig stor gruppe av materielle kriterier er de som berettiger behandling av opplysninger dersom det er *nødvendig* for de tilhørende formålene.[550] Det kan stilles spørsmål ved hvorvidt det også ligger en prosessuell komponent i denne typen nødvendighetskriterier. Den databehandlingsansvarlige må ta stilling til hvorvidt den materielle berettigelsen er holdbar, altså om nødvendighetskriteriet er innfridd. Selv om et nødvendighetskriterium forutsetter en reell evaluering, noe som i en viss forstand er en prosess, er det vesentlige forskjeller mellom dette og et samtykke fra den registrerte. Berettigelsen og dens rekkevidde kan avklares på forhånd, og spørsmålet om nødvendighet har i prinsippet et endelig svar. Utgangspunktet er at den databehandlingsansvarlige evaluerer nødvendighetskriteriet unilateralt. Dersom tilsynsorganet skulle overprøve den databehandlingsansvarliges vurdering, vil det fremdeles ligge en forutsetning til grunn om at det finnes ett svar på det konkrete spørsmålet om nødvendighet som er mer korrekt enn andre mulige svar. En materiell berettigelse kan fastslås ensidig, mens en prosessuell berettigelse innebærer at vilkåret for å behandle opplysninger innfris gjennom en enighet mellom parter.

Samtykke er et begrep som er definert både i helseregisterloven og personregisterloven.[551] Terskelen for at et samtykke skal gi holdbar berettigelse for å behandle opplysninger er relativt høy. Prosessuell berettigelse for behandling av personopplysninger kan ikke baseres på et implisitt eller hypotetisk samtykke. De tre kvalifiserende elementene i legaldefinisjonen er frivillig, uttrykkelig og informert. I tillegg må ordet erklæring anses som et krav om at samtykket er tilstrekkelig klart signalisert, selv om det ikke nødvendigvis ligger et dokumentasjonskrav i det. Personverndirektivet har en lignende definisjon av samtykke.[552] Direktivets definisjon omfatter i tillegg det kvalifiserende elementet «spesifikk», som kan forstås som et krav om å angi grensene hvilken rekkevidde samtykket har.

Elementet «frivillig» forbyr selvfølgelig bruk av tvang. Videre, i følge Helsinkideklarasjonen, som er omforente etiske prinsipper for medisinsk forskning, skal hver potensiell

[549] Personopplysningsloven § 8 annet komma, og § 9(1)(b).
[550] Personopplysningsloven § 8(1)(a-f), og § 9(1)(c-h).
[551] Definisjonene er praktisk talt likelydende: «en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv.» Personopplysningsloven § 2(1)(7), helseregisterloven § 2(1)(11). «Opplysninger» er erstattet med «helseopplysninger» i helseregisterlovens ordlyd.
[552] EP/Rdir 95/46/EF artikkel 2(1)(h), «den registrertes samtykke»: enhver frivillig, spesifikk og informert viljesytring om at den registrerte gir sitt samtykke til at personopplysninger om vedkommende blir behandlet.

forskningsdeltaker også ha «the right to abstain from participation in the study or to withdraw consent to participate at any time without reprisal.»[553] Det å kunne trekke et samtykke tilbake er en nødvendig egenskap ved et frivillig samtykke.[554] Retten til ikke å samtykke, uten at det skal føre negative konsekvenser, sikrer at samtykket er reelt frivillig i slike situasjoner som er sammenlignbare med å delta i medisinsk forskning. Overgangen fra medisinsk behandling til medisinsk forskning innebærer en kvalifisert endring av formålet, og det er ingen grunn til at det å avstå fra å samtykke til det nye formålet skulle påvirke rettigheter, tjenester eller forventninger som er knyttet til det opprinnelige formålet med behandlingen av opplysninger. At det ikke skal føre til negative konsekvenser har imidlertid sine grenser. En prosessuell berettigelse ville være meningsløs dersom frivillighet tolkes slik at den registrerte ikke skal oppleve noen negative konsekvenser dersom han heller ikke vil samtykke til å behandle opplysninger innenfor det opprinnelige formålet. Hvis det var tilfelle, kunne ikke et samtykke ha tilbudt noe som helst bredere adgang til å behandle opplysninger enn det som allerede tillates ut fra en materiell berettigelse.

At samtykket skal være uttrykkelig, og at det er en erklæring, viser til at et samtykke må signaliseres på en eller annen måte.[555] Erklæring innebærer at den registrerte har en subjektiv hensikt om å signalisere samtykke. Kravet til uttrykkelighet vil ikke nødvendigvis innebære mer enn at samtykket ikke kan være hypotetisk eller implisitt. Det er ikke i direkte forstand et dokumentasjonskrav, til forskjell fra for eksempel Helsinkideklarasjonen, som krever at samtykket skal være skriftlig eller bevitnet eller på annen måte gjenstand for nærmere angitte formaliteter. Sett i sammenheng med en funksjon som berettigelse etter personopplysningsloven §§ 8 og 9, må likevel den databehandlingsansvarlige påse at samtykket faktisk er gitt. Dersom en prosessuell berettigelse er det vilkåret som berettiger behandlingen, er det vanskelig å anse berettigelsen som holdbar dersom det er tvil om at samtykket faktisk har vært signalisert.

«Informert samtykke» er kanskje i særlig grad det begrepet som forbindes med Helsinkideklarasjonen. Deklarasjonen inneholder en katalog over hvilken informasjon som må meddeles den potensielle forskningsdeltakeren. Vel så viktig er presiseringen av at den legen som gjennomfører forskningen er forpliktet til å skaffe og formidle riktig og tilstrekkelig informasjon. Samtykket er ikke informert før pasienten har forstått hva det innebærer. Kravet til at samtykket må være informert, i personopplysningslovens og helseregisterlovens defini-

[553] World Medical Association: «Declaration of Helsinki».
[554] Dette har senere blitt kodifisert i helseforskningsloven § 16.
[555] Deryck Beyleveld og Roger Brownsword (2007): *Consent in the law*, s. 188ff.

sjoner, må antas å ha omtrent tilsvarende betydning som den mer detaljerte fortegnelsen i Helsinkideklarasjonen.

Personopplysningsloven aksepterer villig både prosessuell og materiell berettigelse. Dette gjelder både for sensitive og ikke-sensitive opplysninger. De ulike artene av berettigelse befinner seg, i hvert fall etter lovens ordlyd, i samme plan.[556] Likevel er det en utbredt oppfatning innen personvernteori at samtykke er, eller i hvert fall bør være, den foretrukne berettigelsesformen for behandling av personopplysninger. En av de tidlige teoretikere innen personopplysningsvern i elektroniske systemer pekte på «the control we have over information about ourselves» som en nøkkelegenskap.[557] Den tyske konstitusjonsdomstolen fastslo en rett til informasjonsmessig selvbestemmelse (*Informationelle Selbstbestimmung*) i en kjent avgjørelse fra 1983, som gjaldt informasjon som ble samlet inn og prosessert av offentlige myndigheter i en nasjonal folketelling.[558]

I forarbeid til helseregisterloven ble det poengtert at samtykke skulle være hovedregelen for helseregistre.[559] Helseregisterloven kan, ut fra den tolkningen Personvernnemnda har gitt av helseregisterloven § 5 tredje ledd, sies å rangere berettigelsesgrunnlagene slik at samtykke har en forrang fremfor nødvendighetskriterier.[560] Saken gjaldt et forskningsprosjekt der Datatilsynet mente at det var behov for å angi krav til samtykke som vilkår for konsesjon, mens klageren mente at det burde være dekning for materiell berettigelse ut fra nødvendighetskriteriene. I den prinsipielle drøftingen av om samtykke anses å ha forrang som berettigende vilkår, tolket Personvernnemnda helseregisterlovens bestemmelse slik at den innebærer en rangering av de berettigende grunnlagene.[561] Det at en slik rangering finnes, etter Personvernnemndas syn, utelukker imidlertid ikke at nødvendighetskriteriene kan være tilstrekkelige. Klageren fikk likevel medhold, ut fra Personvernnemndas samlede vurdering.

Dekningen for å innfortolke en rangering av de berettigende grunnlagene vil antakelig være svakere for personopplysningsloven §§ 8 og 9 enn for helseregisterloven § 5. I en utredning skrevet på oppdrag for Justisdepartementet og Moderniseringsdepartementet, som

---

[556] Det samme gjelder for berettigelse etter personverndirektivet artikkel 7, «[procedural and substantial justifications are], as it were, on the same plane.» Beyleveld og Brownsword (2007), s. 337.
[557] Alan F. Westin (1967): *Privacy and freedom*
[558] Saken er blant annet omtalt i Giovanni Sartor (2006): «Privacy, Reputation, and Trust: Some Implications for Data Protection». I: *Trust Management*, s. 354–366.
[559] Ot.prp. nr. 5 (1999-2000). En intensjon om at samtykke skal være hovedregelen er nevnt flere steder. Hoveddrøftingen av dette er på s. 141–142. Flere høringsinstanser hadde bemerket at lovforslaget ikke fulgte opp denne intensjonen tilstrekkelig tydelig.
[560] PVN-2004-01, forskningsprosjekt ved Statens arbeidsmiljøinstitutt.
[561] «… at alternativet med nødvendighetsbegrunnelser ikke er likestilt med samtykke, slik at den behandlingsansvarlige står fritt til å velge en nødvendighetsbegrunnelse av rene hensiktsmessighetsbetraktninger fremfor å bygge på samtykke.» PVN-2004-01.

ledd i evaluering av personopplysningsloven, ble det foreslått endringer i disse bestemmelsene. De foreslåtte endringene stadfester, og markerer tydelig, en slik rangering i trinnhøyder, der lovhjemmel og samtykke er primære rettslige grunnlag, mens nødvendighetskriterier er sekundære grunnlag.[562] Personverndirektivets artikkel 7 signaliserer imidlertid fremdeles ingen slik rangering.

Tilsynelatende gir mulighetene til å samtykke, eller til å la være å samtykke, den registrerte makt til å utøve kontroll, men det er også reist innvendinger mot samtykkets egnethet og berettigelseskraft. I en anbefaling fra 2007 advarer artikkel 29-gruppen mot å basere legitimeringen av elektroniske pasientjournaler utelukkende på samtykke fra de registrerte.[563] I dokumentets kapittel II, paragraf 4(a)(aa), anbefaler de at «reliance on consent should be confined to cases where the individual data subject has a genuine free choice.» Tilrådningen er at materiell berettigelse bør være hovedregelen.

Noen innsigelser mot hvor egnet samtykke er, som uttrykkes på ulike vis, er faren for at det blir en innholdsløs formalitet uten reell frivillighet, at den registrerte selv mister oversikten, og at robust håndtering av samtykker er ressurskrevende. En enda mer alvorlig innvending går ut på at samtykke kan være en dårlig erstatning for en samfunnskontroll i form av en prosess for å undersøke hvor langt den materielle berettigelsen rekker:

> [O]ne of the recurrent themes of our discussion has been that legal systems are prone to fictionalize consent, that is, to proceed as though A has consented when this manifestly is not the case. This is much worse than a distortion of the facts or sloppy practice; it avoids addressing the need for substantive justification – and, of course, the most worrying case is where a faux procedural justification is offered in lieu of a failed substantive justification (or one that would fail).[564]

Selv om berettigelse basert på samtykke har en relativt sterk posisjon som «hovedregel» i helseregisterlovgivningen, finnes det også tegn til svekket tro på hvilken egnethet det har for formålet. Et konkret tegn er det økende antallet nasjonale helseregistre som baseres på lovhjemmel som materiell berettigelse.[565] Det blir også anført argumenter om den betydningen kompletthet i registrene har for forskningskvaliteten, som grunn for at flere registre bør unntas fra krav til samtykke.[566]

---

[562] Schartum og Bygrave (2006), s. 87–89.
[563] *Working Document on the processing of personal data relating to health in electronic health records (EHR)*
[564] Beyleveld og Brownsword (2007), s. 338.
[565] Det har vært en moderat, men jevn økning av sentrale helseregistre som er personidentifiserbare og ikke basert på samtykke, hjemlet i helseregisterloven § 8(3).
[566] Et strategidokument om felles teknisk og organisatorisk plattform for helseregistre, som også skal favne medisinske kvalitetsregistre, gir en bred drøfting av spørsmålet «hvorfor kan ikke alle helseregistre være basert på samtykke?» *Gode helseregistre – bedre helse*, s. 50.

Når videreformidlingen av helseopplysninger mellom IT-systemer og mellom virksomheter med stor sannsynlighet vil øke betydelig i helsesektoren, er det likevel ikke egentlig spørsmålet om hvorvidt man foretrekker prosessuell eller materiell berettigelse som er det viktigste. Flettverket av ulike former for berettigelser i forskjellige situasjoner kan kanskje være et større problem. Konsekvensene for den registrerte kan bli en ugjennomtrengelig og uforutsigbar floke av ulike grunnlag for behandlingen. Når aktørene blir mange, og behandlingene mer komplekse, er det en fare for at en lang rekke av vekslende typer berettigelse fører til at selv godt opplyste borgere vanskelig kan holde oversikt og vite hva et konkret samtykke, eller en annen handling vedkommende foretar seg for å påvirke behandlingen av opplysninger, egentlig innebærer og fører til.

6.2.3.3 Berettigelse for videre bruk og videreformidling av helseopplysninger

Behovet for å evaluere om behandlingen av helseopplysninger fremdeles er berettiget, vil melde seg hver gang det skjer noe som har betydning for det gjeldende grunnlaget. Ulike omstendigheter kan forårsake at et reelt behov for å behandle helseopplysninger beveger seg bort fra eller ut over den berettigelsen som var vurdert eller innhentet i utgangspunktet. Det er to generelle typer av slike situasjoner, som er noe ulikt regulert. Den ene er å bruke opplysningene til formål som er uforenlige med det opprinnelige formålet, enten i egen eller i en annen virksomhet. Den andre typen situasjon er videreformidling av helseopplysninger til en annen virksomhet, når formålet ikke er uforenlig med det opprinnelige formålet.

Bruk av helseopplysninger for andre og uforenlige formål krever alltid den registrertes samtykke, uavhengig av om den opprinnelige behandlingen har hatt en materiell eller en prosessuell berettigelse.[567] Ved videreformidling til en annen virksomhet er ikke samtykke nødvendigvis påkrevd, den nye behandlingen skal ha sin egen berettigelse, som i prinsippet kan være uavhengig av hvilken berettigelse som gjelder i virksomheten som avgir opplysningene. Hvorvidt det er behov for materiell eller prosessuell berettigelse er en ny vurdering. Mens den opprinnelige innsamlingen av opplysninger kan ha vært basert på en materiell berettigelse, enten at det er fastlagt i lov eller adgang til det ut fra et nødvendighetskriterium, kan bruk i en virksomhet som opplysningene overføres til kreve prosessuell berettigelse. Det kan imidlertid også være motsatt, opprinnelig innsamling basert på den registrertes samtykke kan gi opphav til videreformidling der mottakerens behandling er basert på en materiell berettigelse. Ved videreformidling av opplysninger, er det behov for holdbart berettigende

[567] Dette følger av personopplysningsloven § 11(1)(c), og av helseregisterloven § 11(3).

grunnlag både hos den databehandlingsansvarlige virksomheten som gir opplysningene fra seg, og hos den databehandlingsansvarlige virksomheten som mottar opplysningene.[568]

Kriteriet «uforenlig formål» er en særskilt restriksjon, som også finnes i personverndirektivet. I direktivets fortale er dette kriteriet omtalt slik at det kan forstås som en barriere mot utglidning, der behandlingen av opplysninger gradvis mister forankringen i den opprinnelige berettigelsen.[569] Etter de norske lovene vil et uforenlig formål utløse et krav til å innhente samtykke, etter direktivet er det i prinsippet ikke adgang til det overhodet.[570] En interessant og stringent måte å tolke dette kriteriet på, lånt fra en analyse av direktivet, er å sette det opp som følgende logiske slutningsrekke: «Let us say that process P2 is compatible with Purpose P1, if the data subject could, on the basis of his knowledge of P1, reasonably expect P2. If we accept this, we would say that P2 is incompatible with P1 if the data subject could, on the basis of P1, reasonably expect process P2 would not be undertaken.»[571] Tolkningen av hva som er et forenlig formål, er nye formål som det kan være rimelig å forvente ut fra kunnskap om opprinnelig formål. Slutningen derfra til at et uforenlig formål er noe som det er rimelig å forvente at *ikke* skal skje, er ganske uproblematisk. Denne tolkningen tilsier en forholdsvis romslig, men ikke uendelig tøyelig, forståelse av hvor stor avstanden mellom formålene kan være før de betraktes som uforenlige.

Slutningen om at formålet er uforenlig hvis det er rimelig å forvente at behandlingen for det nye formålet ikke finner sted forenkler tolkningsarbeidet, til å gjelde et spørsmål om hvorvidt koblingen mellom forenlighet og den registrertes rimelige forventninger er en holdbar premiss. En slik kobling kan vanskelige leses direkte ut av direktivet eller den norske lovgivningen, men begrepet rimelige forventninger er godt etablert i internasjonal personvernteori.[572] Det er en målestokk som bringer inn den registrertes personvern, både gjennom hensynet til forutberegnelighet og hensynet til beskyttelse som er uavhengig av hvor opplysn-

---

[568] Berettigelsen er imidlertid ikke en transitiv egenskap, $A \rightarrow B \rightarrow C \neq A \rightarrow C$. Det vil si at dersom A kan videreformidle opplysninger til B, og B igjen kan videreformidle opplysninger til C, innebærer ikke det nødvendigvis at videreformidling direkte fra A til C har en holdbar berettigelse, $A \rightarrow C$ må vurderes på eget grunnlag.

[569] EP/Rdir 95/46/EF. «Formål for behandlingen som fastsettes etter innsamlingen, må ikke være uforenlige med formålene slik de opprinnelig ble fastsatt» (fortalens avsnitt 28, tredje punktum).

[570] Sitert fra EP/Rdir 95/46/EF artikkel 6(1)(b), første punktum: «Medlemsstatene skal fastsette bestemmelser om at personopplysninger (…) skal innsamles til bestemte, uttrykkelig angitte og berettigede formål samt at senere behandling ikke skal være uforenlig med disse formålene.»

[571] Dag Elgesem (1999): «The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data». I: *Ethics and Information Technology,* s. 283–293.

[572] Begrepet «rimelige forventninger» (reasonable expectations of privacy) har utgangspunkt i en dom i amerikansk høyesterett, *Katz v. United States, 389 U.S. 347 (1967)*. Denne doktrinens betydning for å forme moderne personvernteori er beskrevet blant annet i artikkelen Frank M. Tuerkheimer (1993): «The underpinnings of privacy protection». I: *Communications of the ACM,* s. 69–73.

ingene befinner seg, som et selvstendig formål som kan avveies mot grunner som tilsier behandling for et nytt formål.[573]

I tillegg til at det antakelig er generelt romslig hva som er forenlige formål, er det direkte angitt i loven at senere behandling av personopplysningene for historiske, statistiske eller vitenskapelige formål ikke anses uforenlig med de opprinnelige formålene.[574] Dermed skal det sannsynligvis mye til for at annen behandling av helseopplysninger innen helsetjenesten og helseforvaltningen er uforenlig med formålet. Det kan være mulig å tenke seg mer sannsynlige scenarioer for uforenlige formål når helseopplysninger formidles til virksomheter utenfor helsesektoren. Et eksempel kunne være at opplysninger til politiet om at en pasient kan være farlig, fordi han har truet en tredjeperson, gir et spor i etterforskningen av den truede tredjepersons lysskye transaksjoner. Det vil imidlertid ligge litt på siden av avhandlingens vektlegging av regulære informasjonsstrømmer. Noe mer aktuelt er spørsmålet om å innhente pasientjournalopplysninger for å kontrollere helsepersonells refusjonskrav. Dette er behandling av opplysningene som for så vidt følger en kjede av materielle berettigelser, men hvor det likevel kan være grunn til å tenke seg at det fra pasientens side er rimelig å forvente at journalopplysninger ikke utleveres til et forvaltningsorgan som skal kontrollere om helsepersonellet har utferdiget riktige refusjonskrav. Spørsmålet om hva pasienten kan forvente når helseopplysningene er samlet inn med det formål å kontrollere behandlerne, har også vært drøftet fra andre synsvinkler. Sivilombudsmannen har i en sak om et slikt spørsmål kommet frem til at pasienten har partsrettigheter, etter forvaltningsloven, når behandleren må utlevere vedkommendes pasientjournal for å kontrollere behandleren.[575]

Det finnes også, for enkelte av de sentrale helseregistrene, forskriftsfestede begrensninger for bruk og videreformidling av opplysninger, som ikke er knyttet til hvorvidt formålet skal anses som forenlig eller ikke. Et eksempel på dette er bestemmelser som forbyr utveksling av helseopplysninger selv om den registrerte skulle ønske å samtykke til det.[576] Flere forskrifter inneholder en bestemmelse med denne ordlyden: «Opplysninger om enkeltindivider som er

[573] I en utredning om hvorvidt romavlytting er i strid med Grunnloven § 102, er også den samme dommen, *Katz v. United States,* brukt som argument for en formålsorientert tolkning av behovet for å ivareta den enkeltes personvern. Alf Petter Høgberg og Marius Stub (2009): «Er reglene om bruk av tvangsmidler i avvergende og forebyggende øyemed forenelige med forbudet mot husinkvisisjoner i Grunnloven § 102?». I: *NOU 2009:15, Skjult informasjon – åpen kontroll, vedlegg 3,* s. 420–449.

[574] Personopplysningsloven § 11(2). Samme angivelse finnes i personverndirektivet artikkel 6(1)(b).

[575] Somb-2008-18.

[576] Personverndirektivet har en bestemmelse som gir medlemsland anledning til å avskjære muligheten for at den registrerte kan samtykke til behandling av de særlige typene opplysninger, herunder helseopplysninger, som er omfattet artikkel 8, i EP/Rdir 95/46/EF artikkel 8(2)(a). Generelt gir dette punktet i artikkelen adgang til å behandle opplysninger dersom den registrerte samtykker, «… med mindre det i medlemsstatens lovgivning er fastsatt at forbudet nevnt i nr. 1 ikke kan oppheves ved at den registrerte gir sitt samtykke.»

fremkommet ved behandling av data etter forskriften, kan ikke brukes i forsikringsøyemed selv om den registrerte selv har anmodet om eller samtykker til det.»[577]

Kriteriet om at et nytt formål ikke skal være uforenlig med det opprinnelige fungerer som en skranke mot helt tilfeldig eller veldig kreativ gjenbruk av opplysninger. Det klart største volumet av utveksling og gjenbruk av helseopplysninger som foregår og kommer til å foregå på tvers av virksomheter og informasjonssystemer dreier seg imidlertid om bruk til forenlige, og oftest nært beslektede, formål.

6.2.4 Plikter til å ivareta nødvendige garantier

«Nødvendige garantier», et begrep som brukes flere steder i personverndirektivet, er her en samlebetegnelse for den litt store og formløse gruppen av tiltak som en databehandlingsansvarlig må sørge for at blir ivaretatt. De nødvendige garantiene er systematisk sett frakoblet spørsmålet om berettigelse. Garantiene er kjøreregler og forpliktelser som prinsipielt gjelder etter at berettiget behandling av helseopplysninger er påbegynt.

Av de bestemmelsene som kan sies å høre inn under betegnelsen nødvendige garantier er noen av pliktene unilaterale, de involverer prinsipielt bare den databehandlingsansvarlige, og dennes eventuelle oppdragstakere. Den databehandlingsansvarlige skal gjøre sin behandling av opplysninger kjent og forståelig, og ivareta tilstrekkelig opplysningskvalitet og informasjonssikkerhet, uavhengig av om noen av de registrerte velger å gjøre bruk av sine rettigheter overfor den ansvarlige. En egenskap ved det som kan betegnes som unilaterale plikter er at den registrerte ikke kan frita den databehandlingsansvarlige fra dem. Den registrerte kan heller ikke frasi seg rettigheter som følger av disse pliktene. Hvorvidt krav til informasjonssikkerhet og kvalitet ivaretas godt nok er et emne for tilsyn og samfunnskontroll, ikke for den enkeltes medvirkning.

Enkelte andre garantier er bilaterale, slik at den databehandlingsansvarliges plikter dreier seg om å imøtekomme krav, ønsker eller valg fra den registrerte. For eksempel vil det at en person gjør bruk av retten til innsyn i opplysninger som er registrert om ham, utløse den databehandlingsansvarliges plikt til å gi innsyn.[578] Andre slike garantier, i personverndirektivet og personopplysningsloven, er bestemmelsene om supplering, retting og sletting av gale eller mangelfulle opplysninger.[579] Den registrertes adgang til å utøve medbestemmelse, over

[577] Jf. bl.a. forskrift om forsvarets helseregister § 1-5(2) og kreftregisterforskriften, 21. desember 2001 nr. 1477 § 1-4(2).
[578] Personopplysningsloven § 18(2), og helseregisterloven § 22.
[579] Personopplysningsloven § 27, og helseregisterloven § 26.

berettiget behandling av opplysninger, er prinsipielt uavhengig av om grunnlaget som berettiger behandlingen er hjemmel i lov, samtykke eller nødvendighetskriterier.[580] Skillet mellom unilaterale og bilaterale garantier dreier seg om grad av medbestemmelsesmulighet. Det er imidlertid nødvendig å presisere at en type rettighet for den registrerte av og til kan bestå av en kombinasjon av forskjellige typer garantier. For eksempel står den enkeltes rett til innsyn, som en bilateral garanti, i sammenheng med visse unilaterale plikter som den databehandlingsansvarlige har til å informere den registrerte, av eget tiltak, om behandlingen av opplysninger.[581] Korrigering, supplering og sletting av opplysninger som er mangelfulle, uriktige, eller som det ikke er adgang til å behandle, skal også utføres av « … den databehandlingsansvarlige av eget tiltak eller på begjæring av den registrerte.»[582]

Personopplysningsloven og helseregisterloven legger i vesentlig grad opp til at de ulike «nødvendige garantiene», enten de er unilaterale eller bilaterale, skal realiseres gjennom virksomhetens internkontrollsystem.[583] Begge lover inneholder to overordnede bestemmelser om dette. Den ene plikten gjelder tiltak som ivaretar tilfredsstillende informasjonssikkerhet, som i all hovedsak er en unilateral garanti.[584] Den andre plikten er en generell internkontrollplikt, til å «etablere og vedlikeholde planlagte og systematiske tiltak for å oppfylle kravene i eller i medhold av denne loven», som vil omfatte det som skal til for å ivareta både unilaterale og bilaterale garantier.[585] Internkontroll er en fleksibel reguleringsmetode, og den innebærer både et stort handlingsrom og en stor grad av definisjonsmakt for den databehandlingsansvarlige.

6.2.4.1 Generelle krav til informasjonssikkerhet

Den relativt detaljerte føringen om tilgangskontroll som er utgangspunkt for avhandlingens problemstilling, at tilgang «kan bare gis i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt»,[586] må ses i sammenheng

[580] En analyse av personverndirektivets innslag av selvbestemmelse skiller begrepet selvbestemmelse i to kategorier rettigheter for den registrerte. Den typen selvbestemmelse som tilsvarer *bilaterale garantier* i teksten her, er rett til medvirkning som gjelder «even after agreeing to the treatment of one's own information». Sartor (2006), s. 355.
[581] Personopplysningsloven §§ 19–22, og helseregisterloven §§ 23 og 24.
[582] Jf. helseregisterloven § 26(1)(1).
[583] Jf. den generelle redegjørelsen for risikobasert internkontroll som reguleringsmetode, kapittel 4.
[584] Helseregisterloven § 16, og personopplysningsloven § 13.
[585] Helseregisterloven § 17, og personopplysningsloven § 14.
[586] Helseregisterloven § 13(1) annet punktum.

med lovens generelle krav til et internkontrollbasert styringssystem for informasjonssikkerhet, for å sikre opplysningenes konfidensialitet, integritet og tilgjengelighet.[587]

Et slikt styringssystem er i hovedsak basert på én bestemt internasjonal standard for sikkerhetsadministrasjon.[588] Denne standarden er også metodisk rammeverk for informasjonssikkerhetsarbeid i flere andre sammenhenger enn sikring av personopplysninger, for eksempel kan industribedrifter velge å la seg sertifisere etter denne standarden uten at sikkerhetsarbeidet er relatert til behandling av personopplysninger. Utarbeiding av virksomhetens kriterier for hva ansatte og eventuelle andre skulle ha tilgang til, og iverksetting og etterlevelse av disse kriteriene, er et sentralt element i denne standarden. I likhet med andre typer sikkerhetstiltak er også tilgangskontrollen underlagt et syklisk, risikobasert styringssystem.

En tidligere versjon av denne standarden var også modell for Datatilsynets retningslinjer for informasjonssikkerhet, gitt i medhold av den dagjeldende personregisterloven.[589] Den tidligere retningslinjen i medhold av personregisterloven hadde imidlertid lite preg av å være et regelverk, det var mer innrettet som sikkerhetsfaglige fremgangsmåter. Med personopplysningsloven og personopplysningsforskriften, og deretter helseregisterloven som trådte i kraft året etter, ble imidlertid standardens overordnede metodikk integrert i loven og forskriften.[590] Overført til forskrift har standardens metodikk i større grad blitt utformet som regulering, og er dermed tilsvarende mindre detaljert sikkerhetsfaglig. Forskriftsteksten henviser ikke eksplisitt til standarden for sikkerhetsadministrasjon.

Det er klart ut fra personopplysningsforskriften § 2-8 at den databehandlingsansvarlige skal styre og ha kontroll med hva medarbeiderne skal kunne bruke informasjonssystemet til, og hvilke tilganger som skal tildeles. Utover det at plikten plasseres, gir ikke bestemmelsen noen nærmere holdepunkter for den databehandlingsansvarliges normsetting – det fastlegges gjennom den databehandlingsansvarliges eget styringssystem, basert på egen vurdering av og aksept av risiko.

---

[587] De tre aspektene ved informasjonssikkerhet er anført i personopplysningsloven § 13. I helseregisterloven § 16 er også «kvalitet» tilføyd som et fjerde aspekt, dermed er kvalitet anført som hensyn i begge internkontrollbestemmelsene i helseregisterloven, §§ 16 og 17.

[588] Nåværende navn på denne standarden er NS-ISO/IEC 27002, etter et navnebytte som er motivert av et ønske om å samle flere sikkerhetsstandarder under en «27000-serie». Tidligere navn, som var aktuelt da personopplysningsloven trådte i kraft, var ISO/IEC 17799. Den ble opprinnelig utarbeidet som en britisk standard, under navnet BS 7799.

[589] En hjemmel for å gi pålegg om sikring av personopplysninger ble tatt inn i personregisterloven § 8b ved endringslov 12. juni 1987 nr. 55. Endringen var initiert av Datatilsynet, som fant hjemmelssituasjonen for å kunne gi pålegg om å sikre personregistre utilfredsstillende, jf. Ot.prp. nr. 34 (1986-1987), s. 26.

[590] Personopplysningsforskriften er delt inn i flere kapitler, som er utfyllende regler for forskjellige forskriftshjemler i personopplysningsloven. Det er derfor liten grad av sammenheng mellom forskriftens kapitler, de regulerer hvert sitt område. Kapittel 2 regulerer informasjonssikkerhet.

6.2.4.2 Norm for informasjonssikkerhet i helsesektoren

Sikkerhetsnormen, Norm for informasjonssikkerhet i helsesektoren, er utgitt 7. august 2006. På forsiden av dokumentet står det *utgitt med støtte av Sosial- og helsedirektoratet*.[591] «Med støtte av» er kanskje litt for beskjedent, muligens også noe obskurt, ettersom Helsedirektoratet både har ledet arbeidet, arrangerer opplæring og er vertskapsvirksomhet for løpende oppdateringer av underliggende veiledninger, faktaark og støttedokumenter. Formuleringen markerer imidlertid at dette er ment å være en flerparts, konsensusbasert bransjenorm.

Bransjevise adferdsnormer er et begrep som finnes i personopplysningsloven, ved at det inngår i Datatilsynets oppgaver å bistå i utarbeidelsen av dem.[592] Loven gir ikke selv noen nærmere anvisning på hva som ligger i begrepet «bransjevise atferdsnormer». Det er ikke plassert i en slik sammenheng at det er knyttet til plikter for virksomheter som behandler personopplysninger, verken i form av krav til deltakelse eller gjennom insitamenter for de som skulle velge å delta. Begrepet har sin bakgrunn i personverndirektivet, som heller ikke bidrar med mange holdepunkter for hva dette er ment å være.[593] Direktivets fortale får imidlertid noe tydeligere frem at kan være ønskelig at bransjer med spesielle behov samarbeider om tolkning og operasjonalisering av det personopplysningsrettslige regelverket på sitt område.

> Medlemsstatene og Kommisjonen skal innenfor sine respektive myndighetsområder oppfordre de berørte yrkesmiljøer til å utarbeide regler for hvordan dette direktiv skal anvendes, slik at gjennomføringen av direktivet fremmes, idet det tas hensyn til særtrekk ved behandling av opplysninger på visse områder, og under overholdelse av de nasjonale bestemmelser som er vedtatt for gjennomføringen.[594]

Det kan være en grunn til en forsiktig tvil om det egentlig fullt ut er dekning for å anse sikkerhetsnormen som et eksempel på bransjevise atferdnormer. Innvendingen ville være at den kanskje ligger nærmere et ordinært styringsinstrument fra overordnet myndighet. Sikkerhetsnormens viktigste funksjon er å tjene som grunnlag for avtaler om informasjonssikkerhet

[591] Direktoratets nåværende navn er Helsedirektoratet. Navnet ble endret fra 1. april 2008, etter en justering i oppgaveporteføljen.
[592] Personopplysningslovens § 42(3)(6). «[Datatilsynet skal] gi råd og veiledning i spørsmål om personvern og sikring av personopplysninger til dem som planlegger å behandle personopplysninger eller utvikle systemer for slik behandling, herunder bistå i utarbeidelsen av bransjevise atferdsnormer.»
[593] Etter EP/Rdir 95/46/EF artikkel 27(1) kan atferdsregler regulere særlige forhold på ulike områder, men heller ikke direktivet kobler atferdsreglene til plikt til eller insitamenter for deltakelse. Artikkel 27(2) gjelder nasjonale myndigheters plikt til å gi uttalelse om slike atferdsregler, tilsvarende personopplysningsloven § 42(3)(6).
[594] EP/Rdir 95/46/EF, fortalen, avsnitt 61.

mellom deltakere i Norsk helsenett.[595] Det stilles i personopplysningsforskriften sikkerhetsbestemmelser krav til avtale som regulerer ansvars- og myndighetsforhold, der avtalens funksjon er at «[d]en behandlingsansvarlige skal ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører, og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet.»[596] Når tilslutning til og etterlevelse av sikkerhetsnormen stilles som vilkår for å bruke en monopolisert kommunikasjonskanal innen sektoren, er det et slags logisk brudd med at den databehandlingsansvarlige bestemmer både formål og hvilke hjelpemidler som skal brukes – her kontrollerer hjelpemiddelet brukeren, og ikke omvendt. En annen måte å uttrykke denne innvendingen på, er at sikkerhetsnormens system er designet som, og henter legitimitet fra, en konsortiummodell, mens det er grunn til å spørre om den ikke reelt sett fungerer mer som en sentralisert styringsmodell.[597]

Et argument for likevel å anerkjenne sikkerhetsnormen som et omforent fellesprodukt, basert på tilslutning fra ulike aktører i sektoren, er at den har vært ment som det, og har vært utarbeidet med bistand fra Datatilsynet i tråd med ovennevnte punkt i Datatilsynets mandat. Utkastene som ble forelått før offisiell utgivelse i august 2006 ble da også underkjent av Datatilsynet, først og fremst fordi de ikke kunne stille seg bak normdokumentets foreslåtte regler om tilgangskontroll.[598]

Spørsmålet om sikkerhetsnormens formelle status kan ha en viss betydning for hva som anses som legitime måter å endre den på, og i hvilken grad det er nødvendig med, og i så fall aksept for, sanksjoner mot de som ikke etterlever den på en overbevisende måte. Et mer vesentlig poeng i denne sammenheng er likevel de sikkerhetsfaglige føringene sikkerhetsnormen uttrykker, særlig innen tilgangskontroll. Sikkerhetsnormen er, i all hovedsak, en utdypning og detaljering av personopplysningsforskriften kapittel 2. Den består av et hoveddokument, der det som kan betraktes som egentlige atferdsnormer ligger. I tillegg er det utarbeidet en rekke veiledninger andre støttedokumenter, med egne identifikatorer og utgivelsesdatoer, som beskriver, forklarer og utdyper ulike sikkerhetsfaglige emner. Sikkerhetsnormen kan betraktes som et «halvfabrikat» risikobasert internkontrollsystem, hovedinnretningen i sikkerhetsarbeidet er de samme metodetrinnene som i personopplysningsforskriften. Et av de største problemene med risikobasert internkontroll som reguleringsmetode, er at

[595] Norsk helsenett er et lukket, elektronisk nettverk for helsesektoren, med relativt høy grad av sikkerhet. Det forvaltes av et eget statsforetak, Norsk Helsenett SF, som er heleid av Helse- og omsorgsdepartementet.
[596] Personopplysningsforskriften § 2-15.
[597] De alternative styringsmodellene konsortium og sentralisering er tidligere omtalt i kapittel 5.2.2.5.
[598] Datatilsynet var representert i styringsgruppe for normen siden oppstarten i 2003, og stilte flere krav, deriblant til tilgangskontroll, for å gi normen sin tilslutning i tråd med personopplysningsloven § 42(3). Jf. *Norm for informasjonssikkerhet i helsesektoren – Datatilsynets vurdering.* (2006).

metoden i liten grad bidrar til felles og harmoniserte mål og kriterier for aksept av risiko.[599] Den databehandlingsansvarlige må selv gjennomføre egen fastlegging av mål, egne risikovurderinger, beslutninger om og iversetting av risikoreduserende tiltak, oppfølging av etterlevelse og avvikshåndtering. Det metodetrinnet som kan kalles å fastsette kriterier for aksept av risiko blir imidlertid underlagt en viss felles normering gjennom sikkerhetsnormen.

De felles atferdsnormene, som i volum utgjør en relativt beskjeden del av sikkerhetsnormen, angir noen felles kriterier for aksept av risiko, riktignok på et relativt overordnet nivå, slik at mange virksomheter antakelig vil se et behov for å detaljere og konkretisere kriteriene noe mer. Disse kriteriene er knyttet til de fire aspektene ved informasjonssikkerhet som skal ivaretas, og i den ustrekning der er nødvendig må balanseres mot hverandre, konfidensialitet, integritet, tilgjengelighet og kvalitet.[600] Kriterier for aksept av risiko er angitt i noen få punkter under hver av disse aspektene.[601] Disse kriteriene dreier seg delvis om å beskytte opplysningene mot virksomhetseksterne angripere, det gjelder blant annet dette punktet under konfidensialitet: «Personer utenfor virksomheten uansett ressurser og kunnskap skal ikke kunne få tilgang til helse- og personopplysninger.» Flere av kriteriene dreier seg imidlertid om å beskytte opplysningene mot uautorisert tilgang innenfor virksomheten, for eksempel dette punktet under konfidensialitet: «Personer innenfor virksomheten skal kun få tilgang i henhold til fastsatte prinsipper for tilgangsstyring i henhold til pkt. 5.2 nedenfor.» Et kriterium for integritet dreier seg om at verken personer i eller utenfor virksomheten skal kunne endre helseopplysninger uten autorisasjon.

De «fastsatte prinsippene» for tilgangsstyring er i stor grad føringer om at virksomheter selv må utforme interne regler, og noen nærmere angivelser av hva slike regler bør omfatte. Det dreier seg blant annet om å forankre interne regler for å tildele tilganger i den ordinære linjeledelsen, om en generell forventning om at det bør finnes tekniske, implementerte kontrollmekanismer for å sikre at de interne reglene overholdes, og om å konkretisere hva medarbeidere kan og ikke kan gjøre som databrukere.

I tillegg til overordnede føringer for virksomhetsinterne regler angir også normen noen egne, mer håndfaste regler. Disse er interessante både fordi de går noe på tvers av det ellers relativt fleksible selvreguleringsregimet, og fordi de er særegne for helsesektoren som virk-

[599] Her vises til den generelle analysen av risikobasert internkontroll i kapittel 4, og særlig til drøftingen av virksomhetsgrenser som problem i kapittel 4.5.3.
[600] Av disse fire aspektene, som er nevnt i sammenheng i helseregisterloven § 16, er det de tre første man finner igjen i standarden NS-ISO/IEC 27002 og i personopplysningsloven § 13. At det siste, *kvalitet*, er med i kravet til informasjonssikkerhet er en særegenhet ved helseregisterloven, som også er inkludert i sikkerhetsnormen.
[601] Sikkerhetsnormen s. 12–13.

somhetsområde. Den første av disse reglene gjelder det å gi annet helsepersonell tilgang til opplysninger, som må være basert på en medisinsk beslutning.

> Bare *autorisert* personell kan få *tilgang* til *helse- og personopplysninger*. *Tilgang* skal gis etter en konkret beslutning basert på at det er iverksatt eller skal iverksettes tiltak for medisinsk behandling av pasienten.[602]

Kravet til at det bare skal være mulig å videreformidle eller skaffe seg tilgang til helseopplysninger når det foreligger en beslutning om tiltak, peker på medisinske behandlingsforløp som et av tilgangskriteriene. Det er en type kriterium som har en utpreget dynamisk karakter, og som stiller relativt høye krav til definert og systematisert beslutningsgrunnlag, et grunnlag som også må holde høy datakvalitet for å fungere effektivt og betryggende i praktisk tilgangskontroll.[603] Dette kravet kan betegnes som faglig offensivt, og må kunne sies å ha beveget seg temmelig raskt fra «tegnebrettet» og inn i en regulatorisk kontekst, uten særlig forutgående faglig og teknologisk modning.

Et annet, begrep, som får en tydeliggjort regulatorisk ramme gjennom sikkerhetsnormen er det som der kalles «nødrettstilgang».[604] Det er en adgang databrukeren har til selvautorisering, innen visse rammer. Dette begrepet har vært innarbeidet i praksis også før sikkerhetsnormen, i noen tilfeller under andre betegnelser som for eksempel den greie metaforen «blålystilgang». Nødrett betegner generelt en straffrihetsgrunn, altså slik at man ikke kan straffes for en ellers forbudt handling hvis den etter omstendighetene er nødvendig.[605] Det har vært antatt, siden lenge før IT-systemenes inntog i helsevesenet, at det må være mulig å bryte taushetsplikten uten at det medfører straff, dersom det vil være farlig for pasienten ikke å bryte den.[606] At brudd på taushetsplikten kan være straffrie når de etter omstendighetene er nødvendige, er i seg selv lite problematisk og neppe kontroversielt. Det er imidlertid et par grunner til å se nærmere på likheter og forskjeller mellom et strafferettslig nødrettsbegrep, anvendt på helsepersonell som opplever et konkret behov for å bryte taushetsplikten, og begrepet «nødrettstilgang» som er en overføring av dette behovet til en virksomhetsorientert informasjonssikkerhetsregulering.

---

[602] Sikkerhetsnormen s. 16, originale uthevinger. Uthevede ord i normen er definert i dens første kapittel. Sikkerhetsnormens bruk av begrepet «tilgang» ligger nærmere måten ordet «videreformidling» er brukt på i avhandlingen, mens «tilgang» ellers i avhandlingen ligger nærmere normens definisjon av «autorisasjon».

[603] Dette er en av flere modeller for tilgangskriterier som gjennomgås og vurderes i avhandlingens kapittel 9.

[604] Definert i sikkerhetsnormen, s. 3: «Med *'nødrettstilgang'* menes i *normen* en *tilgang* hvor prinsippene for tilgangsstyring ikke blir fulgt, fordi det for å avverge fare eller skade er behov for øyeblikkelig *tilgang* til *helse- og personopplysninger*, og dette ut fra de foreliggende omstendigheter må vurderes som rettmessig.»

[605] Straffeloven [1902] § 47.

[606] For eksempel av Olaf Trampe Kindt (1952): «Lægens taushetsplikt». I: *Norsk retstidende,* s. 961–967, som skriver at man ut fra «nødstilstandsbetraktninger» kunne være berettiget til å bryte sin taushetsplikt for å hjelpe eller redde mennesker eller økonomiske verdier.

Et moment som tyder på at nødrettsbetraktningene får en annen karakter når de overføres til regulering av virksomhetens sikkerhetsarbeid, er at nødrettstilganger blir noe som virksomheten tilrettelegger for. Den enkelte ansatte gis da en mulighet for å autorisere seg selv, dersom vedkommende ut fra de forhåndsdefinerte tilgangskriteriene ikke har tilgang til nødvendige opplysninger. Det er ikke lenger den som har taushetsplikten som bestemmer seg for at det er konkrete omstendigheter som gjør det nødvendig å bryte den. I praksis er det den som trenger opplysningene, og ikke den som sitter med dem, som beslutter at dette er nødvendig. På hvilken måte, i hvilken utstrekning, og for hvilke opplysninger det skal være mulig å autorisere seg selv, er en del av den rammen virksomheten etablerer og overvåker. Nødvendigheten er så å si planlagt og innkalkulert.

Et annet moment, som følger av sikkerhetsnormen, er at virksomheten skal føre kontroll og ettersyn med hvordan denne nødrettstilgangen brukes.[607] Etter det generelle utgangspunktet om nødrett som straffrihetsgrunn, vil det være det helsepersonellet som har taushetsplikt, og som finner det nødvendig å bryte den, som kan påberope seg nødrett. Dersom det er grunn til å tvile på at det var berettiget å bryte taushetsplikten på et slikt grunnlag, vil den vurdering helsepersonellet gjorde ut fra omstendighetene kunne prøves.[608] Ved et tilrettelagt opplegg for nødrettstilgang blir dette noe mer komplisert: Databrukeren som autoriserer seg selv svarer for sine handlinger overfor virksomheten, mens virksomheten skal kunne dokumentere og bevise sin kontroll med det samlede opplegget for nødrettstilganger overfor tilsynsorganet, i tråd med prinsippene for samfunnskontroll med internkontrollsystemer. Denne totrinns etterprøvingen er hensiktsmessig for å håndtere et visst volum av bruken av et slikt opplegg for nødrettstilganger, men det er mer tvilsomt hvor godt det harmoniserer med prinsippet om nødrett som straffrihetsgrunn.

Betegnelsen «nødrettstilgang» kan dermed ses på som et litt uheldig navn på en nødvendig mekanisme. Et strukturert opplegg for selvautorisering, underlagt virksomhetens kontroll, burde antakelig heller hatt et eget grunnlag – og kanskje et mer treffende navn – for å passe inn i den måten informasjonssikkerhet ellers reguleres på. Det er et opplegg som en virksomhet bør kunne velge, når den gir et bedre resultat enn andre metoder de kunne ha valgt.

[607] Sikkerhetsnormen, s. 12: «*Nødrettstilgang* kan etableres som en mulighet for *autoriserte* brukere til å gi seg selv *tilgang* uten å følge fastsatte prinsipper (…) I så tilfelle må det utarbeides egne rutiner for dette. Begrunnelsen for *nødrettstilgang* skal dokumenteres og hvert enkelt tilfelle skal følges opp som et *avvik*.»
[608] Jf. straffeloven [1902] § 47.

6.2.4.3 Rettigheter og muligheter for medbestemmelse

Den registrertes medbestemmelse og kontroll, i en eller annen form, inngår i ulike sammenhenger som et av de grunnleggende personopplysningsrettslige prinsippene.[609] Med det som utgangspunkt, gir personopplysningsloven og helseregisterloven den registrerte et relativt beskjedent knippe muligheter for medbestemmelse under og etter behandling. Den registrertes rettigheter etter personopplysningsretten, og pasienters rettigheter til å utøve medbestemmelse over behandlingen av helseopplysninger etter helseretten, er på enkelte områder sammenfallende. De helserettslige bestemmelsene er til dels mer detaljerte, og vil i praksis kunne ha større betydning for hvordan tilgangskriterier kan og bør uttrykkes enn det som er tilfelle for rett til medbestemmelse etter personopplysningsretten.[610]

Blant eksemplene på bilaterale garantier er den registrertes rett til innsyn og til å korrigere opplysninger nevnt ovenfor.[611] Dette er garantier som gir muligheter for medbestemmelse, men som likevel ikke vil ha direkte betydning for hvordan tilgangskriterier kan eller bør uttrykkes. En personopplysningsrettslig bestemmelse, der valg som den registrerte kan treffe vil ha betydning for tilgang og videreformidling, er sperring av opplysninger.

> Den registrerte kan kreve at helseopplysninger som behandles etter §§ 5, 7 og 8, skal slettes eller sperres, dersom behandling av opplysningene føles sterkt belastende for den registrerte og det ikke finnes sterke allmenne hensyn som tilsier at opplysningene behandles. Krav om sletting eller sperring av slike opplysninger rettes til den databehandlingsansvarlige for opplysningene.[612]

Den registrerte kan kreve at opplysninger skal sperres fra et ikke-behandlingsrettet helseregister, dersom opplysningene føles sterkt belastende.[613] Det forutsettes altså verken at opplysningene er gale, overflødige, eller at behandlingen av dem har vært uberettiget. Dersom den registrerte får medhold i et ønske om å slette opplysningene, vil de være ute av registeret og dermed ha liten betydning for videre tilgang formidling. Opplysninger som sperres, i stedet

---

[609] Nærmere belegg for medbestemmelse og kontroll som et grunnleggende prinsipp i personopplysningsretten, finnes i Bygrave (2002), s. 63–66. I Bygraves systematikk er dette prinsippet ivaretatt gjennom ulike typer regler: Samtykke som prosessuelt vilkår før behandling, unilaterale plikter til å informere den registrerte og samfunnet for øvrig, og gjennom en tredje og siste type, bilaterale medvirkningsmuligheter under og etter behandling, som er den relevante typen her.

[610] De relevante helserettslige bestemmelsene presenteres nærmere i kapittel 6.3 nedenfor.

[611] I kapittel 6.2.4.

[612] Helseregisterloven § 28(1). Henvisningen til §§ 5, 7 og 8 fungerer som en angivelse av at dette gjelder ikke-behandlingsrettede helseregistre. Etter § 28(3) skal krav om sletting i behandlingsrettede helseregistre avgjøres etter helsepersonelloven § 43.

[613] I høringsutkast til helseregisterloven var kriteriet opprinnelig «belastende», men ble i proposisjonen endret til «sterkt belastende», som altså hever terskelen noe for å få innvilget sletting eller sperring på dette grunnlaget. Ot.prp. nr. 5 (1999-2000), s. 287.

for å slettes, vil derimot bli værende i registeret, og konsekvensen av at de er sperret må håndteres på et eller annet vis.

Både helseregisterloven og dens forarbeider bruker begrepet sperring, stilt opp som et likeverdig alternativ til sletting, men uten at det følger noen nærmere beskrivelse av hva sperring skal innebære i praksis. En temmelig kort, og relativt vag, formulering finnes i et forarbeid til den generelle personopplysningsloven: «'Sperring' kan innebære både et forbud mot å bruke opplysningene uten samtykke fra den registrerte, samt krav om å etablere nødvendige tekniske foranstaltninger for å hindre at opplysningene brukes.»[614] Å hindre bruk av opplysninger uten at de slettes er en rimelig forståelse av ordet sperring. Et annet tolkningsmoment er å skjele til hva som menes med sperring av *behandlingsrettede* helseregistre. Man har ikke en egentlig positiv hjemmel for å kreve sperring av journal eller annet behandlingsrettet helseregister.[615] En rett til å få journalen sperret blir likevel innfortolket i retten til å motsette seg at taushetsbelagte opplysninger gis til samarbeidende helsepersonell.[616] Det er en speilvending av det presumerte samtykket. «Sperring» har relativt lang fartstid som et operativt uttrykk for at en pasient har valgt å bruke sin rett til å motsette seg at opplysninger deles med samarbeidende helsepersonell:

> I slike tilfeller snakker man om sperring av journal. I praksis foretas sperringen ved at det på journalomslaget anmerkes at journalen ikke skal utleveres uten pasientens samtykke. Risikoen som er forbundet med at behandlende lege/sykehus på grunn av slik sperring ikke har alle relevante opplysninger om pasienten tilgjengelig, må vedkommende pasient selv ta på sin kappe. Pasienten må imidlertid informeres om mulige konsekvenser av sitt standpunkt.[617]

Denne måten å sperre journal på er praktisert både for papirjournaler og elektroniske journaler. I en elektronisk journal er det ikke et fysisk omslag som merkes, men en representasjon av de rutiner virksomheten har valgt for å håndtere sperringen. Sammenlignet med sperring i et ikke-behandlingsrettet helseregister, etter helseregisterloven § 28, er det to forskjeller som er verdt å merke seg. Den første er at den formelle terskelen for å velge sperring er lavere i det

---

[614] NOU 1997:19, s. 212. Det fremheves at dette er en ny betydning av sperring, som ikke fantes i den tidligere personregisterloven. (Ellers dreide NOU-ens betraktninger om sperring seg primært om videreføring av bestemmelsen i personregisterloven § 8a om å kunne sperre sitt navn mot utsending av direktesendt reklame. En slik bestemmelse ble tatt inn i personopplysningsloven § 26, men er gjeldende fra 1. juni 2009 tatt ut av personopplysningsloven, og flyttet over i den nye markedsføringsloven, 9. januar 2009 nr. 2).

[615] Sperring etter helseregisterloven § 28 gjelder bare ikke-behandlingsrettede helseregistre, og henvisningen videre til helsepersonelloven § 43 for behandlingsrettede helseregistre omfatter bare sletting, og ikke sperring.

[616] Jf. helsepersonelloven § 25(1).

[617] Bente Ohnstad (1991): «Taushetsplikt og utlevering av pasientjournal». I: *Tidsskrift for Den norske lægeforening,* s. 2317–2319. En bestemmelse om presumert samtykke til å dele opplysninger med samarbeidende helsepersonell fantes den gang i legeloven [1980], § 45 jf. § 34.

behandlingsrettede registeret. Pasienten kan motsette seg at opplysninger gis til samarbeidende helsepersonell uten å begrunne det med at opplysningene føles sterkt belastende. Den andre forskjellen er at sperringen knyttes til enkeltvise brukssituasjoner, i stedet for en totalvurdering av hvor belastende helseopplysningene er i seg selv. Dermed blir medbestemmelsen mer fleksibel, ved at pasienten kan velge å lette på sperringen i hver enkelt situasjon hvor det kan være aktuelt. Sperring i et ikke-behandlingsrettet helseregister kan bare innføres, og eventuelt heves, for opplysningene som sådan, uten at det er formelt eller praktisk mulig å endre dette fra situasjon til situasjon.

Eksempelet med sperring er interessant fordi det illustrerer viktige forskjeller mellom personopplysningsrettslige og helserettslige regler om behandling av helseopplysninger. Medbestemmelse etter personopplysningsrettslige regler dreier seg ofte om å få gjennomført enkle og grunnleggende justeringer. Krav om dette rettes til den databehandlingsansvarlige virksomhet, og vil kunne være gjenstand for vurderinger der den registrertes krav blir veid mot tunge samfunnshensyn. Beslutninger som springer ut av et ønske om å utøve medbestemmelse er ikke gjenstand for hyppige endringer, de er forholdsvis statiske, og dermed også relativt enkle å representere elektronisk. Som en mer generell observasjon, er det relativt få bestemmelser som gir den registrerte rett til å påvirke behandlingen av opplysninger, dersom behandlingen i utgangspunktet er berettiget. Å ivareta den registrertes interesser og rettigheter under og etter behandling er i overveiende grad basert på unilaterale garantier, og samfunnskontroll med virksomhetens egne kontrollprosesser.

De helserettslige reguleringene som gir pasienten en større eller mindre grad av rett til eller mulighet for medbestemmelse over behandlingen av helseopplysninger er mer fleksible, mer dynamiske og mer fragmenterte. I eksemplet med sperring av journal er dette noe som pasienten kan praktisere ulikt i forskjellige situasjoner, det kan variere for eksempel med pasientens egen opplevelse av hvor følsomt et bestemt helseproblem er, eller hvilken tillit han har til det ene eller det andre helsepersonell. At medbestemmelsen er mer dynamisk innebærer at den kan være mer kompleks å representere elektronisk, og mer sårbar for både uheldige kombinasjoner av valg fra pasientens side og svakheter i representasjonens kvalitet. Sist, men ikke minst er det relativt stor detaljrikdom i de helserettslige reglene om behandling av helseopplysninger. Pasientens medbestemmelse inngår i ulike sammenhenger med andre regler, der både helsepersonell og virksomhet har ulike plikter, friheter og rettigheter.

Den personopplysningsrettslige reguleringen tilbyr virksomhetene relativt stor grad av frihet til å beslutte egne tilgangskriterier, mens adgangen til medbestemmelse egentlig er mer beskjeden enn reguleringens idégrunnlag skulle tilsi. Den helserettslige reguleringen av

behandling av helseopplysninger fremstår på sin side som så opptatt av å være både konkret og nyansert, at det kan være vanskelig å oppnå tilgangskriterier som er tilstrekkelig stabile og overskubare til at de lar seg representere, iverksette og kontrollere systematisk.

6.3 Helserettslige regler om behandling av opplysninger

Personopplysningsrettens regler ivaretar behandling av opplysninger som sådan, med plikter for hver virksomhet som behandler dem. Helseopplysningene kobles fra den medisinske behandlingen, og håndteres etter egne regler for å sikre opplysningene. Helserettens regler om behandling av opplysninger kan betraktes som mer direkte knyttet til helsehjelpen, og til det helsepersonell som er involvert i helsehjelpen, prinsipielt uavhengig av om behandlingen er innen samme virksomhet eller ikke. Fra et helsehjelpsperspektiv er det ikke alltid mulig eller ønskelig å betrakte helseopplysningene som frakoblet fra den medisinske behandlingen. Både pasientens egen kunnskap om sin situasjon, og kunnskapen om og kontrollen med hvem som får vite hva, vil kunne bli en del av pasientens samlede opplevelse av helsehjelpen og sin egen helsetilstand. Retten til å informeres om sin tilstand, på en måte pasienten selv forstår, er et sentralt element i pasientrettighetene.[618] Informasjon kan holdes tilbake fra pasienten dersom det ut fra en medisinsk vurdering av fare for pasienten er «påtrengende nødvendig», terskelen er altså temmelig høy. Terskelen er litt lavere for å unnlate å informere hvis det er av hensyn til andre som står pasienten nær, da må det være «klart utilrådelig» å informere.[619] I en fagbok om medisinsk etikk tar forfatteren til orde for å se den informasjon legen gir pasienten som integrert i behandlingen:

> Legens informasjonsplikt overfor pasienten innebærer likevel ingen plikt til å gi alle pasienter all informasjon om deres sykdom og helsetilstand. Det kunne i noen tilfeller virke mot sin hensikt. Legen må ha *doseringsansvar* ikke bare med hensyn til medikamenter, men også når det gjelder informasjon til pasienten.
> Det er minst to sider ved dette doseringsansvaret. For det første: Hvor mye informasjon skal pasienten ha, og når skal informasjonen gis? For det andre: På hvilken måte skal informasjonen presenteres? Fremdeles går atskillig pasientkritikk mot leger nettopp ut på at doseringsansvaret for informasjon til pasientene ikke forvaltes tilfredsstillende.[620]

[618] Pasientrettighetsloven § 3-5.
[619] Pasientrettighetsloven § 3-2(3).
[620] Knut Erik Tranøy (2005): *Medisinsk etikk i vår tid*, s. 118 (original utheving). Sitatet viser også den uavklarte spenningen mellom autonomiprinsippet og paternalisme, som er kommentert et annet sted i samme bok (s. 52).

Den helserettslige reguleringen av behandling av helseopplysninger forener og balanserer en rekke ulike hensyn gjennom detaljerte regler i formell lov. Sammenlignet med den virksomhetsorienterte personopplysningsretten, ligger den helserettslige reguleringen av behandling av helseopplysninger generelt nærmere pasienten, og nærmere individuelt helsepersonell og de enkelte helsehjelpssituasjonene. Regelverket innholder rikelige andeler av både bestemte plikter, rom for skjønn og rom for medbestemmelse. Det betyr ikke nødvendigvis at det vil være uklart, eller vanskelig å finne ut av, hva som er rett behandling av opplysninger i hvert enkelt tilfelle. Det kan imidlertid innebære et behov for et detaljert beslutningsgrunnlag før man kan avgjøre om en person kan gis tilgang til bestemte opplysninger.

Dersom man skal representere tilgangskriteriene basert på de helserettslige reguleringene, i helsetjenestens og helseforvaltningens ulike IT-systemer, betyr det at representasjonene må bygges på tolkninger av enkeltheter i rettskildene. Det er i utgangspunktet en annerledes innfallsvinkel enn de personopplysningsrettslige kravene til informasjonssikkerhet, der det først og fremst stilles krav til at virksomheten selv beslutter tilgangskriterier basert på relativt generelle føringer, og iverksetter tilgangskontroll ut fra sine egne definerte kriterier. På helseregisterlovens område vil den viktigste føringen for de tilgangskriteriene virksomheten skal beslutte være at de er «i samsvar med gjeldende bestemmelser om taushetsplikt», altså et visst innslag av den helserettslige reguleringen.[621] Det er imidlertid relativt åpent hvor detaljert samsvar det er mulig eller hensiktsmessig å oppnå. Videre i dette kapitlet gjennomgås eksemplifiseringer av ulike helserettslige bestemmelser som det kan være mer eller mindre aktuelt å forsøke å representere i en virksomhets tilgangskriterier. I hvilken grad ulike valg av teknologiske prinsipper for å uttrykke og iverksette tilgangskriterier egner seg for å representere de aktuelle helserettslige bestemmelsene vurderes mer konkret i kapittel 9 nedenfor.

6.3.1 Taushetsplikt om helseopplysninger

Legers taushetsplikt har vært hevdet som en yrkesetisk norm siden oldtiden, som en personlig plikt til ikke å røpe det man får vite om en pasient.[622] Legens taushetsplikt var innarbeidet og ble ansett som bindende også før den fikk en konkret lovhjemmel. Taushetsplikten var forutsatt i den tidligere straffeprosessloven, ved at det var særskilte krav til når en leges

[621] Helseregisterloven § 13(1) annet punktum. Dette kravet til samsvar er utgangspunktet for avhandlingens problemstilling, jf. kapittel 1.2 ovenfor.

[622] Opprinnelsen knyttes ofte til «den hippokratiske ed». Denne edens egentlige opphav, hvor autentisk den er, hvor stor vekt den ble tillagt med videre, er et spørsmål for historikere. Her legges ikke mer i henvisningen enn at den yrkesetiske normen anses å ha lenger historie enn rettslige konfidensialitetsnormer.

vitneplikt kunne frita fra taushetsplikten.[623] Straffeloven innførte en bestemmelse om straff for utøvere av en del yrker, deriblant leger, dersom de rettsstridig åpenbarte hemmeligheter som var betrodd dem i stillings medfør.[624] Taushetspliktens helserettslige utgangspunkt, fortroligheten mellom behandler og pasient, også det han «får rede på» uavhengig av pasientens egne betroelser, ble konkret lovfestet i den første legeloven av 1927. En taushetsplikt for apotekerne, og deres medarbeidere, ble imidlertid innført allerede med Christian 5tes forordning av 1672.

> Oc efftersom adskillige Siugdommer forekommer / som Patienterne ey gierne vilde haffve aabenbarede / oc dog aff Recepterne vel kand kiendis oc agtis / da skulle Apoteckerne sambt deris Svenne oc Tiennere saadant holde forborgen / oc ey det udsige eller aabenbare / med mindre nogen merckelig Fare var at befrycte / om det bleff fortiet.[625]

Et interessant trekk ved denne tidlige utgaven av en lovfestet taushetsplikt er at den minner vel så mye om et moderne personopplysningsrettslig regelverk som en profesjonsnorm. Det er ikke de opplysningene som blir værende i relasjonen mellom lege og pasient som er gjenstand for det særskilte beskyttelsesbehovet. Det er den videre behandlingen av resepter, som dokumenterer sykdommene, som begrunner at konfidensialiteten må ha et vern som er uavhengig av lagringsmedium og virksomhetsgrenser. Ikke minst er plikten utvidet til apotekerens medhjelpere, den omfatter alle som vil kunne ha en berettiget tilgang til de skriftlige reseptene.

6.3.1.1 Yrkesmessig og forvaltningsmessig taushetsplikt

Straffeloven innførte to ulike bestemmelser om straff for å krenke taushetsplikter. Den ene er knyttet til bestemte yrker, og de betroelser man får gjennom yrket.[626] Det andre straffebudet gjelder krenkelse av «taushetsplikt som i henhold til lovbestemmelse eller gyldig instruks følger av hans tjeneste eller arbeid for statlig eller kommunalt organ.»[627]

En forskjell mellom den yrkesmessige og den forvaltningsmessige taushetsplikten, som har en viss betydning for behandling av helseopplysninger, er at den forvaltningsmessige taushetsplikten gir en viss generell adgang til å bruke og formidle opplysningene innen

[623] Straffeprosessloven [1887], 1. juli 1887 nr. 5, (Opphevet). Jf. også Anders Færden (1897): «Lægers taushedspligt». I: *Tidsskrift for Den norske lægeforening,* s. 171–187.
[624] Straffeloven [1902] § 144.
[625] Christian 5tes forordning, 4. desember 1672 § 24. Det fremgår av forordningens § 1 at den gjelder «I begge Vore Riger oc Lande».
[626] Straffeloven [1902] § 144. Det betegnes ofte som en yrkesmessig taushetsplikt. Et mer arkaisk synonym er en kallsmessig taushetsplikt, et annet synonym er profesjonsbestemt taushetsplikt.
[627] Straffeloven [1902] § 121. Dette betegnes ofte som tjenestemessig eller forvaltningsmessig taushetsplikt.

samme virksomhet. Denne siden ved forvaltningsmessig taushetsplikt betegnes også som *organintern* taushetsplikt. Det klareste uttrykket for dette er at taushetsplikt ikke er til hinder for «at opplysningene er tilgjengelig for andre tjenestemenn innen organet eller etaten i den utstrekning som trengs for en hensiktsmessig arbeids- og arkivordning, bl.a. til bruk ved vegledning i andre saker.»[628] Den yrkesmessige taushetsplikten er personlig, slik at den ikke åpner for at opplysningene skal være generelt tilgjengelige for andre som arbeider i samme virksomhet.

Det er en viss spenning mellom yrkesmessig og forvaltningsmessig taushetsplikt, som kanskje har kommet tydeligst til uttrykk når noen har reist forslag om å endre innretningen, enten forslaget gjelder endring fra yrkesmessig til forvaltningsmessig taushetsplikt, eller omvendt. Knut Selmer fremmet tidlig et innspill om å tone ned den yrkesmessige taushetsplikten i helsevesenet:

> Den tradisjonelle modell hvor legen og pasienten i prinsippet sitter inne i et lukket rom hvor ingen informasjon kan passere ut gjennom veggen, er ikke lenger tilstrekkelig. En rasjonell modell ville vise legen og hans pasient sittende bak et skjold som hindrer informasjonen i å flyte ut til andre deler av samfunnet. Men mot helsevesenet er det ingen barriere; tvert imot representerer legen innfallsporten til systemet, ikke bare når det gjelder tiltak for behandling og helbredelse, men også når det er tale om innsamling og overføring av relevant informasjon.[629]

Det som lå til grunn for Selmers forslag var ikke et ønske om å svekke taushetsplikten, men om å etablere fungerende rettsregler som stemte overens med reell praksis. Han pekte på at den yrkesmessige taushetsplikten etter dagjeldende lover, gjennom etablert praksis, var overstyrt av teamarbeid og samhandling, og basert på et «fingert samtykke». Mange av de svakhetene han pekte på er tatt hensyn til gjennom konkrete lovhjemler for unntakene senere, selv om man har beholdt den grunnleggende yrkesmessige taushetsplikten.[630]

Selmers forslag om å legge om til noe som ligner mer på forvaltningsmessig taushetsplikt i helsevesenet ble møtt med motbør, blant annet fordi den yrkesmessige taushetsplikten den gang ble sett som en viktig og nødvendig barriere mot et altomfattende, sentralisert helseinformasjonssystem:

---

[628] Forvaltningsloven § 13b (1)(3). Klare hjemler for organintern gjenbruk av opplysninger kom inn i forvaltningsloven med endringslov 27. mai 1977 nr. 40.

[629] Selmer (1977), s. 127. Artikkelen var basert på et foredrag på Helsedirektoratets seminar om EDB i helsevesenet i 1974.

[630] Å gi opplysninger til samarbeidende helsepersonell ble det gitt en generell hjemmel for i legeloven [1980] § 34. Denne bestemmelsen er videreført i helsepersonelloven § 25.

> Selmers taushetspliktsmodell har viktige konsekvenser for mulighetene til å kunne bygge opp medisinske informasjonssystemer. Hvis hans syn på taushetsplikten er juridisk holdbart eller autoriseres av lovgivende myndigheter, er veien åpen for etablering av et gigantisk EDB-basert informasjonssystem som kan inneholde en rekke medisinske opplysninger om alle nordmenn.[631]

Også i utredningen om pseudonyme helseregistre kom utvalget frem til at de hjemlene man hadde for meldeplikter og andre unntak fra taushetsplikten ikke kunne være holdbare for det store omfanget av innrapportering som et sentralt, sykdoms- og skaderegister ville kreve.[632] Utgangspunktet for vurderingene var at det dreide seg om en yrkesmessig taushetsplikt.[633]

For balansens skyld kan det bemerkes at debatten om yrkesmessig eller forvaltningsmessig taushetsplikt ikke bare har dreid seg om å legge om til organinterne prinsipper i helsevesenet. Det har også vært argumentert for at velferdsforvaltningen, der man har mer eller mindre profesjonslignende klientrelasjoner, bør legge om til innretninger som ligger nærmere en yrkesmessig taushetsplikt.[634] I en utredning med forslag til lov som integrerer helse- og sosialtjenester i kommuner, foreslås en omfattende taushetspliktregulering som er satt sammen av elementer av både yrkesmessig og forvaltningsmessig taushetsplikt.[635]

Den formen for taushetsplikt som i overveiende grad gjelder for helsetjenesten og helseforvaltningen er en yrkesmessig taushetsplikt.[636] Et sykehus eller annen helseinstitusjon står derfor ikke like fritt som forvaltningsorganer i andre sektorer til å beslutte tilgangskriterier utelukkende ut fra betraktninger om hensiktsmessig intern organisering. Helt entydig er likevel ikke dette bildet, det finnes visse innslag av organintern taushetsplikt også i den helserettslige reguleringen. Disse innslagene har imidlertid både smalere nedslagsfelt og gjelder mer avgrensede typer situasjoner enn det unntaket for organintern bruk av opplysninger som følger av forvaltningsmessig taushetsplikt. Én slik bestemmelse er tilgang til opplysninger for personell som bistår med elektronisk bearbeiding, eller service og vedlikehold av utstyr.[637] For å medføre et gangbart unntak fra taushetsplikten, må bistanden være nødvendig for å

[631] Asbjørn Kjønstad (1978): «Sosialarbeidernes taushetsplikt». I: *Lov og Rett,* s. 491–509. (s. 488).
[632] Sykdoms- og skaderegisteret var et forslag utredet av Folkehelseinstituttet, og er i hovedsak det som har blitt videreført som Norsk pasientregister.
[633] NOU 1993:22, avsn. 7.3.3. Utvalget vurderte også spørsmålet om vilkår for å opprette registeret kunne være oppfylt, men konkluderte med at de eksisterende bestemmelsene ga «desto mindre grunnlag for å opprette et sentralt register med disse opplysningene.»
[634] Kjønstad (1978).
[635] NOU 2004:18, s. 167–169, utkast til kapittel 9 i forslag til ny lov. Etter denne utredningen har Nav-reformen avstedkommet en egen lov om sosiale tjenester i NAV, 18. desember 2009 nr. 131, der den samme organinterne taushetsplikt gjelder som ellers i NAV. I følge Stortingsmelding nr. 47 (2008-2009), s. 57, «arbeides det med sikte på at det i 2010 skal legges fram forslag til oppfølging av forslagene i NOU 2004:18.»
[636] Helsepersonelloven § 21, gjelder opplysninger og forhold « … som de får vite om i egenskap av å være helsepersonell.»
[637] Helsepersonelloven § 25(2).

oppfylle lovbestemte krav til dokumentasjon. Det forutsettes imidlertid ikke noe personlig fortrolighetsforhold mellom pasienten og personell som yter slik bistand. En annen slik bestemmelse er adgangen den som yter helsehjelp har til å «gi opplysninger til virksomhetens ledelse når dette er nødvendig for å kunne gi helsehjelp, eller for internkontroll og kvalitetssikring av tjenesten.»[638] Det er en temmelig vidtfavnende dreining i retning av organintern taushetsplikt.[639] Nedslagsfeltet «virksomhetens ledelse» innebærer at opplysningene kan brukes i delegerbare oppgaver, og ikke at opplysningene må forbli avgrenset til en personkrets øverst i hierarkiet. Adgangen til å kommunisere pasientopplysninger er imidlertid begrenset til visse formål, og opplysningene skal avindividualiseres så langt det er mulig. Et element av organintern innretning finner man også i plikten helsepersonell har til å gi opplysninger, begrenset til relativt få opplysningstyper, til virksomhetens pasientadministrasjon.[640]

6.3.1.2 Unntak fra taushetsplikten – plikt og frihet til å videreformidle helseopplysninger

I helseretten vil man finne et relativt høyt antall situasjoner der det er gjort unntak fra utgangspunktet om taushetsplikt. Den detaljerte kodifiseringen av unntaksbestemmelser er en relativt ny lovgivningsteknisk utvikling på dette området. Et alternativ til en detaljert kodifisering er en mer åpen og skjønnsmessig såkalt rettsstridsreservasjon.[641] Det vil si at det angis et generelt vurderingskriterium for når det kan være rettmessig å fravike taushetsplikten. I tillegg til mange detaljerte unntaksbestemmelsene inneholder helsepersonellovens taushetspliktbestemmelser også en generell rettsstridsreservasjon, der vurderingskriteriet er tungtveiende interesser.[642] Utover det angitte vurderingskriteriet gir en rettsstridsreservasjon også rom for nødrettsbetraktninger som grunnlag for å fravike taushetsplikten.[643]

Helsepersonellovens systematiske disposisjon av unntak fra taushetsplikten deler disse inn i henholdsvis opplysningsrett, opplysningsplikt og meldeplikt.[644] Enkelte av disse bestemmelsene i helsepersonelloven peker videre til unntak etter andre lover, slik at det reelle antallet

[638] Helsepersonelloven § 26(1).
[639] At bestemmelsen er vidtfavnende tilkjennegis også i forarbeid til loven: «Bestemmelsen gir en videre adgang til å kommunisere pasientopplysninger enn de øvrige unntak i taushetspliktlovgivningen gir hjemmel for.» Ot.prp. nr. 13 (1998-1999), s. 230.
[640] Helsepersonelloven § 26(2).
[641] Ørnulf Rasmussen (1997): *Kommunikasjonsrett og taushetsplikt i helsevesenet*, beskriver en utvikling i legers taushetsplikt fra en vid rettsstridsreservasjon til en betydelig endring i retning av kodifisering. Han observerte at det fremdeles var igjen en «rest av den tidligere rettsstridsreservasjonen» i den daværende legeloven [1980] § 31. Detaljeringsgraden i unntakene økte ytterligere med helsepersonelloven fra 1999.
[642] Helsepersonelloven § 23(1)(4): «[Taushetsplikt etter § 21 er ikke til hinder for:] at opplysninger gis videre når tungtveiende private eller offentlige interesser gjør det rettmessig å gi opplysningene videre.»
[643] Jf. drøftingen av «nødrettstilganger», kapittel 6.2.4.2 ovenfor.
[644] Det fremgår av kapitteloverskriftene i helsepersonelloven, henholdsvis kapittel 5, 6 og 7.

unntak fra taushetsplikten er en god del høyere enn denne delen av helsepersonelloven gir inntrykk av.[645] Selv om opplysningsplikter og meldeplikter har hvert sitt kapittel i loven, er det ingen reell forskjell i den deontiske modaliteten. I begge tilfeller har helsepersonell plikt til å gi opplysninger, og den angitte mottaker har en krav-rettighet til å motta dem.[646] Det kan likevel være praktisk viktige forskjeller mellom opplysnings- og meldeplikter. En meldeplikt innebærer ofte at mottakeren har anledning til å angi formkrav. I tillegg kan man vente et større innslag av rutine og regularitet ved meldeplikter enn ved opplysningsplikter.

Når helsepersonell har en opplysningsrett, står de prinsipielt fritt til å velge å gi opplysninger eller til å la det være. Helsepersonellets frihet innebærer en ikke-rettighet for den som er interessert i å motta opplysningene.[647] I helserettslig teori brukes begrepet taushetsrett som et synonym for opplysningsrett.[648] Den deontiske modaliteten er den samme, begge deler er noe helsepersonell kan gjøre, selv om man muligens ville velge å bruke ordet opplysningsrett i litt andre situasjoner enn der hvor man velger ordet taushetsrett. En så enkel klassifisering av unntakene etter modalitet, hvorvidt man har plikt til eller frihet til å formidle opplysninger, står imidlertid i fare for å tilsløre nyanserikdommen i unntakene fra taushetsplikten.

Den kanskje viktigste faktoren som nyanserer unntaksbestemmelsene, er ulike sider ved pasientens rett eller mulighet til informasjon og medbestemmelse. For eksempel gjelder det en plikt til å gi opplysninger til sosialtjenesten om forhold som «bør føre til tiltak», men etter denne bestemmelsen må pasienten samtykke for at helsepersonell skal ha plikt til å gi videre taushetsbelagte opplysninger.[649] Dersom opplysningen gjelder en gravid kvinnes rusmisbruk, skal derimot sosialtjenesten ha opplysninger om dette uten at det kreves samtykke.[650] Øvrige opplysnings- og meldeplikter gjelder også i overveiende grad uten krav om pasientens samtykke. Det er imidlertid verdt å merke seg at for den mest omfattende bestemmelsen om meldeplikt, som generelt pålegger å sende meldinger til de helseregistrene som er hjemlet i forskrift i medhold av helseregisterloven, vil eventuelt krav til samtykke være avhengig av vilkåret for behandling, altså hvorvidt det aktuelle helseregisteret er samtykkebasert eller ikke.[651] De forskriftshjemlede helseregistrene er imidlertid i liten grad basert på samtykke.[652]

---

[645] En generell henvisning til andre for opplysningsrett finnes i helsepersonelloven § 23 nr. 6, mens meldeplikter etter § 37 vil gjelde alle de meldeplikter som fremgår av helseregisterloven § 9.
[646] Jf. Hohfelds nyanseringer av plikter og rettigheter, kapittel 2.2.1 ovenfor.
[647] Korrelasjonen frihet og ikke-rettighet er et annet av Hohfelds begrepspar, jf. kapittel 2.2.1.
[648] Begrepene angis å ha likt meningsinnhold blant annet i Kjønstad (1978), i Ot.prp. nr. 13 (1998-1999) og i NOU 2004:18.
[649] Helsepersonelloven § 32(1).
[650] Helsepersonelloven § 32(2).
[651] Helsepersonelloven § 37 fastslår at helsepersonell har slik meldeplikt. Tilsvarende plikt, både for virksomheter og helsepersonell, følger av helseregisterloven § 9.
[652] Jf. kapittel 5.2.3 ovenfor.

Den generelle regelen om samtykke, for å løse helsepersonell fra taushetsplikt, går ut på at et slikt samtykke utløser en opplysningsrett, men ikke en plikt.[653] Til forskjell fra helseregisterloven inneholder ikke helsepersonelloven noen definisjon av samtykke som angir hvor tydelig eller konkret det må være. Det forutsettes imidlertid at et samtykke må være tilstrekkelig for formålet. Det vil i de fleste tilfeller innebære at det kreves informert samtykke for å løse helsepersonell fra taushetsplikten. Både presiseringen av at samtykke utløser opplysningsrett, men ikke opplysningsplikt, og forutseningene om samtykkets beskaffenhet, er utførlig omtalt i kommentaren til denne bestemmelsen i lovens proposisjon.[654] Selv om samtykke fra den som har krav på taushet generelt bare utløser opplysningsrett etter denne bestemmelsen i helsepersonelloven, finnes det likevel i annet regelverk situasjoner der samtykke utløser en plikt til å informere: «Dersom pasienten samtykker til det eller forholdene tilsier det, skal pasientens nærmeste pårørende ha informasjon om pasientens helsetilstand og den helsehjelp som ytes.»[655]

En innsigelsesrett, som kan ses som en svakere form for samtykke fordi det er pasienten selv som må ta initiativ for å utøve en medbestemmelse, er i visse tilfelle tilstrekkelig slik at fravær av innsigelser utløser opplysningsrett. Opplysningsrett ut fra dette grunnlaget gjelder når helsepersonell kan ha behov for å gi opplysninger til samarbeidende helsepersonell, fordi det er nødvendig for helsehjelpen.[656] Det finnes imidlertid også en del situasjoner der helsepersonell har opplysningsrett uten at det er gitt noen uttrykt rett til å utøve medbestemmelse. Dette gjelder blant annet for den generelle rettsstridsreservasjonen, og for situasjoner der annen lovgivning fastsetter eller klart forutsetter at taushetsplikt ikke skal gjelde.[657]

Ved siden av de mange variantene av pasientens mulighet til medbestemmelse, er det også to andre faktorer som bidrar til å nyansere det prinsipielle skillet mellom opplysningsplikt og opplysningsrett. Den ene faktoren kan kalles initiering, den andre kan kalles betingelser.[658]

Initiering av en opplysningsplikt er i noen tilfeller en plikt til å gi opplysninger av eget initiativ, i andre tilfeller utløses plikten av at den som har rett til å motta opplysninger ber om

---

[653] Helsepersonelloven § 22(1). At denne bestemmelsen ikke utløser en plikt virker ikke helt opplagt ut fra ordlyden, men det fremgår av forarbeid (jf. neste note) i tillegg til at det følger av lovens systematiske disposisjon, ved at bestemmelsen er plassert i lovens kapittel 5.
[654] Ot.prp. nr. 13 (1998-1999), s. 227–228.
[655] Pasientrettighetsloven § 3-3(1).
[656] Helsepersonelloven § 25(1).
[657] Helsepersonelloven § 23, henholdsvis nr. 4 (rettsstridsreservasjon) og nr. 6 (lovbestemte unntak). Et eksempel på unntak, som gjelder på grunn av at det er forutsatt i lov, er opplysningsrett ved fremming av refusjonskrav til Helfo, folketrygdloven § 22-2, jf. ulike bestemmelser i folketrygdloven kapittel 5.
[658] Grupperingen av disse faktorene er rent pragmatisk. Av hensyn til senere forsøk på å formalisere ulike typetilfeller av unntak fra taushetsplikt (kapittel 8, nedenfor) er det ønskelig å holde antallet faktorer relativt lavt.

dem.[659] Meldepliktene er i større grad initiert av utenforliggende situasjoner eller hendelser, for eksempel fødsel og død.[660] I en viss forstand er meldeplikter mottakerinitiert, fordi det vanligvis er mottakeren som tilrettelegger meldingskanalen og bestemmer formater og eventuelle tidsintervaller med videre for meldingene.

Når helsepersonell har opplysningsrett har ikke en mulig mottaker rett til å få opplysninger, det skal avgjøres av den som har taushetsplikten. Likevel kan man også her skille mellom hvorvidt en mulig mottaker er den som har et motiv for å ønske opplysninger, og tar initiativ til å be om dem, eller om det er helsepersonellet selv som tar initiativet. Å gi opplysninger til samarbeidende helsepersonell, med mindre pasienten motsetter seg det, kan man tenke seg ofte er på initiativ fra den som avgir opplysningene, selv om det også er mulig at en mottaker kan initiere det.[661] Å gi opplysninger om en pasient til et forsikringsselskap skjer i utgangspunktet på mottakerens initiativ, selv om det kan avskjæres både av manglende samtykke og av at helsepersonellet ut fra opplysningsretten velger ikke å gi opplysninger. Mottakerens initiativ vil imidlertid stå sterkt i svært mange tilfeller, ettersom frivilligheten kan være nærmest illusorisk for den som trenger forsikring, og fordi det skal mye til før helsepersonell kan forsvare å overstyre pasientens samtykke til å gi opplysninger.

I eksempelet på en opplysningsrett der pasienten ikke får et reelt tilbud om å utøve medbestemmelse, fremming av refusjonskrav, er det grunn til å spørre om det er friheten til det helsepersonellet som avgir opplysningene som er illusorisk. Den muligheten en behandler har til å la være å gi opplysninger om pasientene, som dokumentasjon av refusjonskravet, kan bare realiseres ved å avstå fra å motta økonomisk oppgjør. Initieringen er i dette tilfellet det økonomiske incitamentet. Selv om eksemplet formelt og systematisk er en opplysningsrett, vil man i realiteten befinne seg nærmere en rettighetsrelasjon av typen plikt/krav-rettighet enn av typen frihet/ikke-rettighet.[662]

Den tredje faktoren som kan sies å nyansere skillet mellom opplysningsrett og opplysningsplikt er de ulike betingelser eller vurderingstemaer en avgiver må ta stilling til for å avgjøre om det skal eller bør gjøres unntak fra taushetsplikten. Disse betingelsene faller grovt sett i tre kategorier. Den ene er ingen betingelser, den andre er spørsmålet om hvilken grad av sannsynlighet det må være for at situasjonen som utløser opplysningsrett eller opplysnings-

[659] Helsepersonell skal varsle sosialtjenesten, etter helsepersonelloven § 32(1), av eget tiltak. Opplysninger skal gis til Helsetilsynet når de krever det, etter § 30. Opplysning til barneverntjenesten skal gis av eget tiltak, etter § 33(2), eller når barneverntjenesten pålegger det, etter § 33(3).
[660] Helsepersonelloven §§ 35 og 36, henholdsvis.
[661] Jf. helsepersonelloven § 25. Utlevering av journal til annet helsepersonell etter helsepersonelloven § 45, som er basert på samme type innsigelsesrett, ble eksplisitt «snudd» fra en avgiverinitiert til en mottakerinitiert innretning ved endringslov 19. juni 2009 nr. 68.
[662] Jf. Hohfelds skjemaer, kapittel 2.2.1 ovenfor.

plikt har inntruffet, den tredje kategorien kan litt mer løselig generaliseres til spørsmål om hvor stor nytteverdi det må ha at opplysningene gis.

Det er først og fremst meldepliktene som tilhører den første kategorien, og ikke påkaller noen vurdering. Det samme er imidlertid også tilfelle for plikten til å gi opplysninger til Helsetilsynet etter anmodning.[663] Også på opplysningsrettens område finnes det eksempler i denne kategorien, selv om det er mer sjelden. Å gi helseopplysninger for å dokumentere refusjonskrav påkaller ingen vurderinger, men som drøftet ovenfor kan det være grunn til å sette spørsmålstegn ved om dette i det hele tatt burde høre hjemme blant opplysningsrettene.

Vurderinger som gjelder grad av sannsynlighet for at det som bestemmelsen dekker har inntruffet, finner er noenlunde likelig fordelt mellom opplysningsrettene og opplysningspliktene. En standardformulering som går igjen er hvorvidt «det er grunn til å tro» at det har skjedd. Det kriteriet gjelder for eksempel ved opplysningsplikt om en gravid rusmisbruker, og ved opplysningsrett om at dyr mishandles eller ikke får godt nok tilsyn.[664] Den plikten lege, psykolog eller optiker har til å melde om at en pasient med førerkort ikke oppfyller de helsemessige kravene som stilles, utløses hvis vedkommende helsepersonell «finner» at det er tilfelle, noe som må bety en vesentlig høyere sannsynlighetsgrad enn «grunn til å tro».[665]

Den tredje kategorien betingelser er mer sammensatt, men kan ses som vurderingstemaer som stiller krav til at det skal være formålstjenlig å gi opplysninger. Slike krav finnes blant opplysningspliktene, for eksempel gjelder plikten til å varsle politi og brannvesen dersom det er «nødvendig for å avverge alvorlig skade på person eller eiendom.»[666] Det er imidlertid mer utbredt, og større behov for slike kriterier, på opplysningsrettenes område. Et tilsvarende nødvendighetskriterium gjelder ved rett til å gi opplysninger til samarbeidende helsepersonell.[667] Andre markører, for eksempel ved noens ønske om å få opplysninger om en avdød person, er at «vektige grunner» skal tale for det om den som ønsker opplysningene ikke er nær pårørende.[668] Dersom det er nærmeste pårørende som spør, skal imidlertid opplysninger gis hvis ikke «særlige grunner» taler mot det.[669] Ut fra den generelle rettsstridsreservasjonen kan det gjøres unntak når «tungtveiende private eller offentlige interesser gjør det rettmessig å

[663] Helsepersonelloven § 30.
[664] Helsepersonelloven §§ 32(2) og § 23(5), henholdsvis.
[665] Helsepersonelloven § 34(1).
[666] Helsepersonelloven § 31.
[667] Helsepersonelloven § 25.
[668] Helsepersonelloven § 24(1).
[669] Helsepersonelloven § 24(2).

gi opplysningene videre.»[670] Den tematiske angivelsen, private eller offentlige interesser, bidrar ikke stort til grensedragningen, men ordet tungtveiende legger terskelen høyt.

Det er altså et bredt spekter av bestemmelser om unntak fra helsepersonells taushetsplikt, og bestemmelsene har så mange ulike nyanser den systematiske disposisjonens skille mellom opplysningsrett og opplysningsplikt kan bli temmelig uskarpt i visse tilfeller.

6.3.1.3 «Snokeforbudet», urettmessig tilegnelse av taushetsbelagte opplysninger

Ved endringslov 9. mai 2008 nr. 34 fikk helseregisterloven og helsepersonelloven nye, nesten likelydende forbud mot urettmessig tilegnelse av taushetsbelagte opplysninger om pasienter. I helsepersonellovens variant er bestemmelsens ordlyd slik:

> Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte opplysninger som nevnt i § 21 uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift.[671]

Hensikten er at de samme opplysningene som er underlagt taushetsplikt, i den forstand at det er forbudt å formidle dem videre til andre, skal det være like lite tillatt å lete frem og lese for egen fornøyelses eller nysgjerrighets skyld. I en mer hverdagslig sjargong er det vanlig å kalle dette «snoking».

Bakgrunn for at dette forbudet ble lovfestet var en sak, der Datatilsynet hadde politianmeldt et helseforetak for mangelfull informasjonssikkerhet.[672] Politiet var enig i vurderingen, og ga helseforetaket et forelegg for brudd på informasjonssikkerhetsbestemmelsen i helseregisterloven § 16.[673] I samme sak ble det reist spørsmål om hvorvidt en avdelingsleder som hadde snoket i journalene hadde brutt sin taushetsplikt, og om vedkommende i så fall kunne straffes for det. Statsadvokaten vurderte dette spørsmålet, og kom til at man ikke kunne innfortolke i helsepersonelloven § 21 et forbud mot å gjøre seg kjent med taushetsbelagte opplysninger, så lenge man ikke bringer informasjonen videre. I en straffesak vil kravet til lovhjemmel stå så sterkt at man ikke bør reise en slik sak selv om det er forståelige reelle hensyn som taler for det.[674] Etter dette kom Helse- og omsorgsdepartementet frem til at det

[670] Helsepersonelloven § 23(4).
[671] Helsepersonelloven § 21a. Tilsvarende bestemmelse finnes i helseregisterloven § 13a.
[672] Her refereres fremstillingen i Ot.prp. nr. 25 (2007-2008), s. 13.
[673] Helseregisterloven § 34(2)(1) hjemler straff for den som forsettlig eller grovt uaktsomt behandler helseopplysninger i strid med §§ 16 eller 18.
[674] Statsadvokaten begrunnet dette med å henvise til Grunnloven § 96.

burde fremgå klart av helselovgivningen at det skal være forbudt å oppsøke eller å sette seg inn i taushetsbelagte pasientopplysninger uten at man har tjenestelig behov for dem.[675]

Det at man vanskelig kunne straffe den enkelte helsearbeider for å lese helseopplysninger uten tjenestelig behov før endringsloven 9. mai 2008 nr. 34, innebar ikke at dette var «tillatt» tidligere. Krav til den databehandlingsansvarliges sikkerhetsarbeid omfattet, og omfatter fremdeles, en plikt til å iverksette ulike tiltak, blant annet relevante begrensninger i den ansattes tilganger, oppfølging av at tilgangene brukes i tråd med fastlagte kriterier, og å sørge for at de ansatte har tilstrekkelige kunnskaper om dette.[676] Virksomheten kan altså straffes for ikke å pålegge sine ansatte relevante og nødvendige restriksjoner. Etter at «snokeforbudet» ble innført kan både virksomheten og den ansatte straffes for slike forhold, den ansatte for den konkrete snokingen, virksomheten for mangelfull informasjonssikkerhet. Begge situasjoner kan være aktuelle, men det kan også være grunn til å være oppmerksom på farene for en mindre heldig dynamikk ved at sanksjonstrusselen rettes mot enkeltansatte. Virksomheter vil kanskje kunne velge økt overvåkning og mistenkeliggjøring av ansatte, i stedet for systematiske forbedringer av eget sikkerhetsarbeid, for lettere å kunne tilbakevise kritikk mot virksomheten.

6.3.1.4 Opplysningsvern for å beskytte andre enn pasienten

Formålet med taushetsplikten etter helsepersonelloven § 21 er å beskytte opplysninger om pasienten. Det finnes imidlertid også andre som vil kunne ha et legitimt behov for vern av opplysninger, som i større eller mindre grad bør ivaretas i virksomhetens informasjons-sikkerhetsarbeid. En type bestemmelser der det kan være aktuelt å beskytte andre personer enn pasienten er de tilfellene der pasientens rett til informasjon, og til innsyn i journal, begrenses av hensynet til noen som står pasienten nær.[677]

Opplysningsvern for å beskytte andre enn pasienten vil imidlertid som oftest være knyttet til andre typer opplysninger enn helseopplysninger. En slik annen type behov for å beskytte opplysninger er de ansattes personopplysningsvern. Noen generelle bestemmelser om virk-somheters adgang til å kontrollere ansattes bruk av virksomhetens informasjonssystem er tatt inn i personopplysningsforskriften.[678] Ulike krav til logging og registrering av ansattes

[675] Ot.prp. nr. 25 (2007-2008), s. 13.
[676] Personopplysningsforskriften § 2-8, jf. helseregisterloven § 16.
[677] Pasientrettighetsloven §§ 3-2(3) og 5-1(2).
[678] Nytt kapittel 9 i personopplysningsforskriften, gjeldende fra 1. mars 2009, jf. personopplysningsloven § 3(4), jf. arbeidsmiljøloven [2005] § 9-5.

handlinger har i utgangspunktet lite direkte med pasienten og helsehjelpen å gjøre, men kan i stigende grad bli et eksternt anliggende ettersom pasienter har fått rett til innsyn i logger.[679]

Det er ikke bare fysiske personer som kan ha behov for opplysningsvern, også informasjonssikkerhetstiltakene som sådan kan trenge noe beskyttelse for å fungere etter hensikten. Derfor er et av kravene i informasjonssikkerhetsreguleringen at virksomheten skal pålegge de ansatte taushetsplikt om informasjon med betydning for informasjonssikkerheten.[680]

En annen og mindre legitim variant av opplysningsvern for andre enn pasienten, er å bruke taushetsplikten, eller bevisste unnlatelser fra dokumentasjonsplikten, til å beskytte seg selv mot kritisk søkelys. Det er ikke pliktsubjektet taushetsplikten er til for å beskytte. Likevel fremmes fra tid til annen mistanken om at det er pliktsubjektets bekvemmelighet som motiverer en ekstra nidkjærhet for taushetsplikten. Formelt sett skal det ikke være særlig anledning til å bruke taushetsplikten til å beskytte pliktsubjektet, ettersom taushetsplikten kan fravikes i den utstrekning pasienten samtykker til det.[681] Det har imidlertid vært påpekt at kompleksiteten i regelverket, og i den faktiske samhandlingen, kan gjøre det vanskelig for pasienten selv å ha reell kontroll med de som behandler opplysningene og deres motiver. I en sosiologisk analyse av taushetspliktens skjulte virkninger, hevdes det at taushetsplikten av slike årsaker til og med kan bli til skade for klienten. Analysen gjelder sosialtjenesten, men kan likevel ha en viss relevans for helsesektoren fordi det dreier seg om et lignende samspill mellom virksomhet, profesjonsutøver og klient som man vil finne i helsetjenesten.

> Hvem er det som taper og hvem er det som vinner på en sterk eller en svak håndheving av taushetsplikten? Taushetsplikten er nemlig ikke et nøytralt instrument, men et middel til å håndtere visse informasjonsstrømmer i samfunnet. Jo mer informasjon og jo viktigere informasjon som underlegges taushetsplikten, desto sterkere instrument til maktutøvelse vil taushetsplikten være. Klientene selv har få eller ingen muligheter til å påvirke taushetspliktens utforming. De avleverer informasjon om seg selv, og de har ikke herredømme over hvordan denne informasjon oversettes, videresendes og eventuelt brukes i nye sammenhenger. De vet ikke at informasjonene brukes som del av et større spill om hvem som skal ha innflytelse i den sosiale sektor, at profesjonene trenger kontroll over informasjonsstrømmene for å sikre sine posisjoner, og at forfordelinger skjules under taushetsplikten slik at tiltak for å rette opp skjevhetene ikke kan settes i verk. Taushetsplikten har en betydning som går langt utover den enkelte klients interesse.[682]

[679] Helseregisterloven § 13(6).
[680] Personopplysningsforskriften § 2-9.
[681] Jf. helsepersonelloven § 22(1).
[682] Else Øyen (1980): «Rammen om taushetsplikten». I: *Taushetsplikt i sosialsektoren*, s. 75–111. (s. 79).

I en annen analyse, fra en helt annen akademisk disiplin, der journaltekster i et psykiatrisk sykehus ble studert, peker forfatteren på at selve dokumentasjonen helsepersonell skriver, måten de skriver den på, kan være slik innrettet at den beskytter og forsvarer institusjonenes verdier fremfor pasientene. Da er perspektivet ikke lenger taushetsplikt og andre regler for å håndtere opplysninger, men at opplysningenes innhold blir slik utformet at de verner den som skriver. Skriveren av journalene er ofte overraskende lojale mot sykehusets prioriteringer og oppfatninger, teksten i journalen som skulle handle om pasienten, handler i stedet om «det forfulgte sykehus».[683]

Tiltak for å unngå bevisste unnlatelser i utøvelsen av dokumentasjonsplikten vil befinne seg i et grenseområde mellom informasjonssikkerhetsarbeid og tiltak for å oppnå bedre opplysningskvalitet.[684] I begge tilfeller vil det kunne være et dilemma at virksomheten, som skal kontrollere seg selv og avdekke problemene, også kan ha mindre legitime og kanskje uuttalte interesser i at problemet ikke blir håndtert.

6.3.2 Pasientrettigheter

De pasientrettighetene som nevnes først i pasientrettighetsloven, i lovens kapittel 2, dreier seg om rett til helsehjelp. Prinsipielt er retten til å bli pasient, og å motta helsehjelp, en annen og mer grunnleggende rettighet enn retten til informasjon og medbestemmelse i informasjonsbehandlingen som følger i lovens kapittel 3, eller innsynsrett etter lovens kapittel 5. Pasientrettighetenes bestemmelser om behandling av opplysninger er i hovedsak en speiling av helsepersonellovens bestemmelser på området, med viktig betoning av behovet for å tilpasse informasjonen til pasientens forutsetninger.

6.3.2.1 Enkelte pasientrettigheter som kan ha betydning for tilgangskriteriene

Blant bestemmelsene om rett til helsehjelp finner man imidlertid også enkelte rettigheter som kan ha en viss betydning for behovene for å behandle helseopplysninger. Retten til fornyet vurdering, gjerne omtalt som en «second opinion», gir pasienten rett til å få en ny vurdering av sin helsetilstand, men bare én gang for samme tilstand.[685] Om en pasient velger å få en fornyet vurdering, kan det innebære at annet helsepersonell trenger tilgang til helseopplys-

[683] Aaslestad (2007), s. 176ff. «Skriveren trekker opp et bilde av en person man må beskytte seg mot; ofte suggereres det at pasienten er en opportunist som tar seg til rette i sykehusverdenen, og som vet å handle fullstendig etter eget forgodtbefinnende.» (på s. 182).
[684] Jf. kapittel 5.1.2 om opplysningskvalitet.
[685] Pasientrettighetsloven § 2-3.

ninger. Pasienten har neppe betenkeligheter med det, ettersom han ønsker denne vurderingen. Likevel er det behov for å finne betryggende måter å gi tilgang for en fornyet vurdering på. Et slikt behov peker i retning av tilgangskriterier som baseres på hendelser og beslutninger i et behandlingsforløp.

En annen rett til helsehjelp, som kan ha betydning for behandling av opplysninger, er retten til en individuell plan for pasienter som har behov for langvarige og koordinerte helsetjenester.[686] Det er en omtrent likelydende bestemmelse i flere forskjellige lover som pålegger organer en plikt til å utarbeide en samordnet, individuell plan. I kommunehelsetjenesteloven er ordlyden slik:

> Kommunehelsetjenesten skal utarbeide en individuell plan for pasienter med behov for langvarige og koordinerte tilbud. Kommunehelsetjenesten skal samarbeide med andre tjenesteytere om planen for å bidra til et helhetlig tilbud for pasientene.[687]

En individuell plan kan inneholde opplysninger som det er behov for å utveksle og håndtere mellom aktører innenfor og utenfor helsetjenesten. Den enkeltes plan skal ha en koordinator, både trekk ved kommunens organisering og trekk ved den enkeltes helsemessige eller sosiale problemer kan ha betydning for om plankoordinatoren representerer helsesektoren eller sosialsektoren. Dermed er det også vanskelig å fastslå generelt både hvor langt helseregisterloven rekker med dens føringer for tilgangskontroll, og hvilke regler som mer generelt skal gjelde for utveksling av opplysninger om pasient/tjenestemottaker.[688] I praksis håndteres individuelle planer ofte med egne IT-systemer som bare inneholder svært begrensede mengder opplysninger om planaktiviteter og involverte aktører. En større nytte av de koordinerte planene forutsetter imidlertid tilstrekkelig felles informasjonsgrunnlag.

Blant pasientrettighetslovens bestemmelser om behandling av opplysninger finnes det også egne rettigheter som ikke kan sies å være klare avspeilinger av plikter i helsepersonelloven. Et eksempel er nevnt tidligere, at pasientens samtykke utløser plikt til å informere pårørende.[689] Et annet eksempel, som i størst grad har kommet på spissen i debatter om bioteknologi, er det

---

[686] Pasientrettighetsloven § 2-5.

[687] Kommunehelsetjenesteloven § 6-2a (1). Andre lover med pliktbestemmelse om å bidra i individuell plan er spesialisthelsetjenesteloven § 2-5, psykisk helsevernloven, 2. juli 1999 nr. 62 § 4-1 og sosialtjenesteloven, 13. desember 1991 nr. 81 § 4-3a. Sammenfallende regler om individuell plan har siden kommet inn i arbeids- og velferdsforvaltningsloven [«NAV-loven»], 16. juni 2006 nr. 20 § 15, og barnevernloven, 17. juli 1992 nr. 100 § 3-2a. I tillegg kan tiltak etter krisesenterlova inngå i individuell plan: «Tilbod og tenester etter denne lova kan inngå som ledd i samordninga av ein individuell plan etter anna lovgiving», krisesenterlova, 19. juni 2009 nr. 44 § 4(2).

[688] Det bør være grunn til å vente et mer samlet og sammenhengende regelverk for slike tilfeller i den varslede oppfølgingen av forslagene i NOU 2004:18, jf. kapittel 6.3.1.1 ovenfor.

[689] Pasientrettighetsloven § 3-3(1), også omtalt i kapittel 6.3.1.2 ovenfor.

som kalles «retten til ikke å vite».[690] Denne rettigheten har relativt lang historie i pasientrettighetssammenheng, blant annet inngår den i Amsterdamerklæringen.[691]

Det bakenforliggende etiske prinsippet er omstridt. Argumentene mot at en slik rett skal finnes er blant annet at det kan være usolidarisk.[692] Resonnementet er at pasienter, enten de mottar helsehjelp eller om de velger å avstå fra visse typer behandling, bør ha en slags plikt til å inngå i det samlede kunnskapsgrunnlaget om helseproblemer og behandling. Retten til ikke å vite kan synes å være en «upopulær» rettighet også i norske miljøer. I en drøfting av de etiske grensene for å påtvinge informasjon, uttrykker forfatteren skepsis til denne rettigheten: «I denne forbindelse har retten til å ikke vite dukket opp. Jeg tror dette er en problematisk innovasjon.»[693] Det problematiske ligger i at en slik rett er vanskelig å speile i en generell plikt for noen til å sørge for å opprettholde pasientens uvitenhet så langt som det ønsket rekker for den enkelte pasient. Også i rettsvitenskapelig drøfting synes det som man er mer opptatt av å markere de begrensninger som må gjelde for en slik rettighet enn å beskrive eller eksemplifisere dens positive anvendelse.[694]

Det finnes imidlertid en nemndavgjørelse, der pasienten fikk medhold i sitt ønske om ikke å vite.[695] Et par hadde søkt om genetisk undersøkelse av befruktede egg før innsetting, fordi det var sannsynlig at den mannlige part kunne ha arvet Huntingtons sykdom fra sin far. Vedkommende ønsket å få gjennomført undersøkelsen av befruktede egg uten selv å få vite om han har sykdommen, fordi han anså en visshet om det som en for stor belastning å leve med. I utgangspunktet ville en snever tolkning av den aktuelle bestemmelsen, om hvem som kan få innvilget slike undersøkelser, forutsette at foreldrenes bærerstatus for en tilstrekkelig alvorlig sykdom er kjent.[696] Et flertall i nemnda kom til at pasientrettighetslovens bestemmelse, om at informasjon ikke skal gis mot pasientens uttrykte vilje, talte for en utvidende tolkning:

---

[690] Pasientrettighetsloven § 3-2(2): «Informasjon skal ikke gis mot pasientens uttrykte vilje, med mindre det er nødvendig for å forebygge skadevirkninger av helsehjelpen, eller det er bestemt i eller i medhold av lov.»
[691] *A Declaration on the Promotion of Patients' Rights in Europe* (1994).
[692] Ruth F. Chadwick (1997): «The philosophy of the right to know and the right not to know». I: *The Right to know and the right not to know*, s. 13–22. Solidaritetsargumentet er interessant som etisk prinsipp fordi innebærer en dreining fra helsepersonellets plikter til en betraktning om at også pasienten har (etiske, ikke rettslige) plikter. I forprosjektrapporten om strategi for helseregistre slås det også til lyd for en dreining, rapporten kaller det riktignok bare en «omformulering», av de etiske prinsippene til å gjelde *pasientens* solidaritet. *Gode helseregistre – bedre helse*, s. 51. Et spørsmål om hvorvidt man bør se for seg at pasienter også skal pålegges rettslige plikter er reist i Kjønstad (2007), s. 38, uten at det forfølges nærmere.
[693] Tranøy (2005), s. 119.
[694] Kun unntak og begrensninger er beskrevet i Syse (2009), s. 268–269. Kildegrunnlaget for påstanden her om motvilje fra rettsvitenskapen er imidlertid tynt, spørsmålet er vesentlig bredere drøftet innen medisinsk etikk enn i juridisk litteratur.
[695] PGD-2008-53, vedtak i preimplantasjonsdiagnostikknemnda, 3. desember 2008.
[696] Bioteknologiloven, 5. desember 2003 nr. 100 § 2A-1.

> Retten til ikke å vite er imidlertid en rettighet som står sterkt. Det faktum at dette ikke drøftes i forbindelse med vedtagelsen av bestemmelser om preimplantasjonsdiagnostikk i bioteknologiloven, kan tyde på at tilfellet hvor en person ikke ønsker å vite sin bærerstatus ikke har vært tenkt på av lovgiver. Dette kan begrunne en utvidende tolkning av ordlyden.

Etter denne sakens spesielle karakter, var det ikke praktiske sett problematisk å imøtekomme pasientens ønske. Dersom man skal ivareta en pasients ønske om ikke å vite, i et heterogent organisert helsevesen, vil det forutsette en høy grad av samkjørte og felles prinsipper for tilgangskriterier, der pasientens valg og beslutninger tas inn som del av kriteriene.

6.3.2.2 Pasientmedvirkning utover pasientrettighetsloven

Fornyet vurdering, individuelle planer og en rett til ikke å vite er etablerte rettigheter under pasientrettighetsloven, og det kan være god grunn til å undersøke hvorvidt disse rettighetene kan eller bør representeres som medbestemmelsesmuligheter i IT-systemers tilgangskriterier. Det kan imidlertid også være verdt å undersøke om det er mulig og hensiktsmessig å tilby pasienter andre elementer av medbestemmelse og valgmuligheter i tillegg, som ikke bygger på direkte lovfestede rettigheter.[697]

Et perspektiv av dette slag er mer dynamiske samtykkekonstruksjoner enn de som følger av personopplysningsretten og helseretten. De strenge kriteriene som oppstilles for at samtykket skal være gyldig kan underminere behovet for deltakelse som er tilpasset pasientens egen takt og mottakelighet. I tillegg til de innvendingene mot informert samtykke på grunn av behov for kompletthet i datagrunnlaget, som er nevnt i kapittel 6.2.3.2 ovenfor, har det også vært reist innvendinger av nærmest motsatt art, som en grunnleggende tvil om det informerte og forutgående samtykkes egnethet som medbestemmelse.

Samtykke er som oftest konstruert som et statisk uttrykk for pasientens vilje. Selv om det er mulig at en annen kan samtykke på pasientens vegne når samtykkekompetansen mangler, er modellen grunnleggende sett slik at *samtykke S* har egenskaper som gjør at det berettiger eller ikke berettiger *handling H*. En annen innfalsvinkel, som særlig har vært fremmet i forbindelse med langvarige pasientrelasjoner, er et mer dynamisk samtykke som pasienten kan endre rekkevidden av ut fra hvordan vedkommende selv opplever ulike situasjoner og egen motivasjon i ulike perioder eller faser. En betegnelse for dette prinsippet, som stammer

[697] Jf. utviklingstrekk i retning av e-helse og mer aktive pasienter, jf. kapittel 5.2.2.4 ovenfor.

fra pionerartikkelen på området, er «forhandlet samtykke».[698] Liknende perspektiver blir også fremmet i mer generell form: «More recent discussions on informed consent have focused on the need to see informed consent as an on-going process rather than as a discrete act of choice that takes place in a given moment of time.»[699] Informasjonssystemer for individuelle planer, og andre systemer der pasienten selv kan justere og endre betingelser for informasjonsbehandlingen, kan betraktes som en mer dynamisk form for samtykke. Denne formen for medbestemmelse kan imidlertid være vanskelig å kombinere med samtykke som personopplysningsrettslig, prosessuell berettigelse for å behandle opplysninger.

6.3.3 Helserettslig regulering av helseopplysninger som representasjonsproblem

Forutsetningen om at tilgangskriterier skal være i overensstemmelse med gjeldende, helserettslige regler om taushetsplikt innebærer at de helserettslige reglene i en eller annen utstrekning bør være representert i tilgangskontrollsystemet.

Bestemmelsene om taushetsplikt er relativt mange og detaljerte. Det behøver ikke i seg selv medføre at det blir vanskelig å utarbeide teknologiske representasjoner. Derimot er det fare for at de mange ulike nyansene i reglene bidrar til at en representasjon blir svært kompleks. En av de nyansene som volder et visst bry er at helsepersonell er underlagt en yrkesmessig taushetsplikt, samtidig som regelverket har visse innslag av forvaltningsmessig taushetsplikt. Ved en ren forvaltningsmessig taushetsplikt ville tilgangskriterier som representerer organisatoriske fullmaktsforholdt ha vært mest nærliggende, mens en yrkesmessig taushetsplikt for eksempel kan tilsi en representasjon av helsehjelpens forløp. Kombinasjoner er krevende.

Unntaksbestemmelsene, tradisjonelt klassifisert som opplysningsrett og opplysningsplikt, er også krevende på grunn av de mange nyansene i disse bestemmelsene. Både ulike grader av medbestemmelse, og ulike vurderingstemaer, påfører de fleste av unntakene et dynamisk element som ofte gjør det vanskelig å avgjøre om det er grunnlag for et unntak eller ikke før det er innhentet opplysninger om situasjonen, og eventuelt om hva pasienten mener.

De ulike innslagene av pasientrettigheter kan også tenkes å danne grunnlag for representasjoner av tilgangskriterier. Det er imidlertid ikke forutsatt i helseregisterloven på samme vis

[698] Dette problemet ble drøftet i den innflytelsesrike artikkelen Harry R. Moody (1988): «From Informed Consent to Negotiated Consent». I: *The Gerontologist,* s. 64–70.
[699] Oonagh Corrigan (2003): «Empty ethics: the problem with informed consent». I: *Sociology of Health & Illness,* s. 768–792. (s. 787).

som representasjoner av taushetsplikt. Pasientrettighetsbaserte ordninger for å styrke medbestemmelsen kan kanskje til en viss grad integreres i tilgangskriterier som representerer taushetspliktbestemmelser, men det kan kanskje være like fruktbart å vurdere egne, mer rendyrkede ordninger for å gi pasienten muligheter til å påvirke informasjonsbehandlingen.

Et av de grunnleggende problemene ved å legge opp til at tilgangskriteriene i stor grad skal representere pasienters medbestemmelse, er at det også vil være nødvendig å håndtere ikkebruk av slike muligheter fra pasientens side. Personopplysningsvernet må fungere også i de situasjoner hvor pasienten velger ikke å være aktiv, og hvor medbestemmelsen er fraværende.

7 Vern av helseopplysninger i praksis

Selv om avhandlingens hovedemne er teoretisk forståelse av regulering av og kontroll med helseopplysninger, og undersøkelse av noen mulige overordnede prinsipper for håndtering av dette, har vern av helseopplysninger også en praktisk side. Denne praktiske siden skal det ikke legges vesentlig vekt på her. Avhandlingens normative ærend, som primært er plassert i del III, tilsier at dersom det kan begrunnes at andre måter å gjøre noe på er bedre, bør praksis endres. En viss kjennskap til og forståelse av praktiske sider ved vern av helseopplysninger har imidlertid vært nødvendig, både for å bygge opp og for å realitetsorientere den teoretiske forståelsen. Denne relativt korte redegjørelsen for noen sider ved vern av helseopplysninger i praksis er dermed til dels en dokumentasjon av noen mellomliggende trinn i prosessen frem til den teoretiske forståelsen. I tillegg vil enkelte momenter fra praksis også kunne inngå som en del av argumentene for hvor hensiktsmessig det ene eller andre teknologiske prinsipp for tilgangskriterier er.

Mange forskjellige spørsmål kan knyttes til praktiseringen av det å verne helseopplysninger. En type spørsmål er om de typer situasjoner som reguleringen gjelder, for eksempel ulike unntak fra taushetsplikt eller pasienter som begjærer innsyn, forekommer hyppig eller sjelden. En annen type spørsmål gjelder relevante aktørers kunnskap om og forståelse av reguleringen. Den siste typen spørsmål dreier seg om holdinger, evne og vilje til å etterleve reglene i tråd med den kunnskapen de har.

Ulike sider ved disse spørsmålene har vært gjenstand for undersøkelser både i Norge og i flere andre land. Det har imidlertid vært vanskelig å finne materiale som knytter praksis til det regelverket aktørene kjenner eller burde kjenne. Derfor er jakten på dokumentasjon av praksis supplert med noen egne undersøkelser, som det redegjøres nærmere for underveis i dette kapitlet. Visse sider ved helsepersonells håndtering av opplysninger ble undersøkt ved å sende ut anonyme spørreskjemaer, mens virksomheters arbeid med å etterprøve hvorvidt ansattes tilgang til helseopplysninger har vært berettiget, er undersøkt gjennom intervjuer med noen få personer som har ulike stillinger inne samme helseforetak. Pasienters erfaringer og forvent-

ninger har ikke vært gjenstand for noen egne undersøkelser i dette arbeidet, på det området er det kun vist til andres funn.

7.1 Pasienters holdninger og ønsker om medbestemmelse

I 2005 gjennomførte Transportøkonomisk institutt to undersøkelser om holdninger til og kunnskaper om personvern på oppdrag fra Moderniseringsdepartementet. Personvernspørsmålene inkluderte, men var ikke begrenset til, helseopplysninger. Den ene undersøkelsen gjaldt virksomheter, den andre befolkningen. Befolkningsundersøkelsen viste blant annet at helseopplysninger er blant de typer opplysninger flest personer oppfatter som sensitivt.[700] Over halvparten var helt eller delvis uenig i at helsepersonell skulle ha anledning til å utveksle helseopplysninger uten samtykke fra pasienten. Samtidig har et stort flertall, 85 prosent, tillit til helsevesenets behandling av personopplysninger. Befolkningens kjennskap til lover og rettigheter er imidlertid lav. Undersøkelsen inneholder også interessante funn om atferd, blant annet at det er relativt få som har bedt om innsyn i opplysninger.[701] Lite bruk av innsynsretten må ses i sammenheng med befolkningens begrensede kunnskaper om rettighetene.

En hovedoppgave ved avdelingen for forvaltningsinformatikk undersøkte hvordan rett til informasjon og innsyn ble håndtert i praksis ved et sykehjem. En del av undersøkelsen dreide seg om pasienters og pårørendes syn på egne rettigheter til og behov for informasjon. Et interessant funn var at dette var viktigere for pårørende enn for pasientene.

> Etter å ha gått gjennom pasienters og pårørendes informasjonsbehov sitter man igjen med et inntrykk av at det er de pårørende som er mest opptatt av rettighetene rundt informasjon og innsyn. Pasientene, som rettighetene automatisk tilfaller etter pasient-rettighetsloven §§ 3-2 og 5-1, viser ikke selv noen interesse for informasjon og innsyn.[702]

Teknologianvendelser som gir pasienter større direkte tilgang til helseopplysningene gjennom egne brukergrensesnitt, der pasientene også gis direkte muligheter for medbestemmelse over opplysningene, er foreløpig så lite utbredt i praksis at man vanskelig kan komme lenger enn

[700] Inger-Anne Ravlum (2005): «Setter vår lit til Storebror … og alle småbrødre med?: Befolkningens holdning til og kunnskap om personvern».
[701] På den annen side viser undersøkelsen av helsepersonells erfaringer, jf. kapittel 7.2.2.1 nedenfor, at over halvparten av helsepersonellet har opplevd at pasienter har bedt om innsyn. Selv om målenivået ikke gjør disse størrelsene direkte sammenlignbare, kan det indikere at bruk av innsynsretten er mer utbredt i helsesektoren enn på andre samfunnsområder.
[702] Ragnhild Bassøe Gunderssen (2005): «Realisering av innsyns- og informasjonsrettigheter ved et sykehjem», s. 83

til å undersøke holdninger til slike anvendelser. I flere europeiske land har man funnet at pasienter har relativt høye forventninger til e-helse, både det å kunne ha mer direkte tilgang til helseopplysninger selv, og å kunne styre selv i mer konkret forstand hvor opplysningene havner og hvem som får tilgang. Pasientenes forventninger om dette står i en viss kontrast til helsepersonells tilbakeholdenhet overfor denne trenden.[703] Da Sverige utredet ny lov om pasientdata, fikk Statistiska Centralbyrån i oppdrag å undersøke hvilke holdninger den svenske befolkningen hadde til ulike e-helsescenarioer.[704] Personer i alderen 20–79 år ble spurt om sin holdning til å etablere sentrale journalsystemer, altså bare en journal for hver pasient nasjonalt. De ble også spurt om synspunkter på det å kunne se egen journal på Internett. Undersøkelsen viste at den svenske befolkningen stiller seg generelt positive til disse scenarioene. Ved en sammenligning mellom den svenske befolkningens syn på disse scenarioene og norsk helsepersonells syn på sammenlignbare scenarioer, viser det seg at helsepersonell er vesentlig mer skeptiske enn pasientene.[705] Helsepersonells skepsis til de scenarioene som gir økt innflytelse til pasienten er større enn skepsisen til scenarioer for sentralisering av opplysninger.

Foreløpig er pasienters praktiske innflytelse over behandlingen av opplysninger relativt beskjeden. For å utøve medbestemmelse over helseopplysningene må pasienten i de aller fleste tilfeller på eget initiativ be om å få utført tydelig konkretiserte handlinger. Det er vanskelig å fastslå med stor sikkerhet om endringer, i form av mer tilrettelegging for at pasienter kan styre informasjonsbehandlingen etter en selvbetjeningsmodell, ville bli brukt i stort omfang til å utøve mer medbestemmelse i praksis. Det er imidlertid grunn til å tro at pasientenes positive innstilling til, og forventninger om, slike innretninger kan bidra til å påvirke utviklingen.

7.2 Profesjonsutøvernes håndtering av helseopplysninger

Helsepersonells håndtering av helseopplysninger kan prinsipielt tenkes som valg mellom handlingsalternativer, som den enkelte treffer. Man kan se for seg tre ulike perspektiver på disse handlingsalternativene. Det ene perspektivet er pasientens uttrykte eller antatte ønsker om hvilke opplysninger som skal gis eller holdes tilbake. Det andre perspektivet er virk-

[703] Andrea Hassol m. fl. (2004): «Patient experiences and attitudes about access to a patient electronic health care record and linked web messaging». I: *Journal of the American Medical Informatics Association,* s. 505–513.
[704] *Din patientjournal: Enkätundersökning.* (2005).
[705] Herbjørn Andresen (2008c): «The Attitude of Norwegian Healthcare Professionals Towards eHealth». I: *The Journal on Information Technology in Healthcare,* s. 429–440.

somhetens og samfunnets krav til, tilrettelegging for, og kontroll med hvordan opplysningene håndteres. Tredje perspektiv er profesjonsnormene, der opplysninger håndteres ut fra profesjonsutøverens egne faglige vurderinger, i kraft av å være helsepersonell, prinsipielt uavhengig av relasjonen til pasient, virksomhet eller samfunn. Ut fra alle de tre perspektivene styres håndteringen av opplysninger av sammensatte etiske, faglige og rettslige normer. Ideelt sett bør perspektivene være resultatlike, slik at helsepersonellets handlingsvalg i en konkret situasjon er det samme uansett om innfallsvinkelen er profesjonen, pasienten, virksomheten eller samfunnet. I de tilfellene hvor forskjellige perspektiver gir forskjellig håndtering av opplysningene som resultat, kan det oppleves som en kollisjon mellom samtidig gyldige plikter.

7.2.1 Ikke-juridiske profesjoners rettsanvendelse

Selv om lovgiver skulle lykkes i å balansere alle hensyn på best tenkelig vis, vil effekten likevel være begrenset dersom regelverket blir for komplisert til at pliktsubjektene klarer å bruke det til å treffe riktige beslutninger. Visse spesielle situasjoner og vanskelige gråsoner kan nok av og til forutsette bruk av juridisk metode, men i hovedsak bør reguleringer være tilstrekkelig forståelige til at de fleste som gjør et arbeid er i stand til selv å overholde reglene uten å konsultere juridisk ekspertise i sine dagligdagse gjøremål. Helsepersonell, som håndterer helseopplysinger i praksis, er som regel ikke samtidig jurister av profesjon.

Innen rettssosiologien har det vært noe forskning på ikke-juridiske profesjoners rettsanvendelse. De arbeidene det er mest relevant å trekke inn her stammer fra et prosjekt om dette fra slutten av 1980-tallet. I hovedsak var det sosialtjenesten, og sosionomene som ikke-juridisk profesjon, som ble undersøkt i dette prosjektet. I en artikkel som oppsummerer mange av funnene i prosjektet nevnes blant annet at disse profesjonsutøverne hadde manglende kjennskap til relevante regelverk og manglende ferdigheter om hvordan regelverket skal anvendes. Videre ble regler oversett når beslutninger ble truffet, i tillegg hadde disse profesjonsutøverne en annen faglig rasjonalitet enn jurister har. Problemet er fremstilt som omfattende, og med stor grad av «delt skyld». Lovgivningen tar ikke tilstrekkelig hensyn til faglige og organisatoriske betingelser. Profesjonsutøverne anses på sin side å ha en tendens til likegyldighet, til og med fiendtlighet, overfor rettssystemet.[706]

[706] Kristian Andenæs (1989): «The law and the nonlegal professionals: on decision-making by medical doctors and social workers». I: *International journal of law and psychiatry,* s. 12.

En annen undersøkelse, fra den amerikanske delstaten Minnesota, kan være interessant å trekke frem fordi den omhandlet om helsepersonells kunnskaper om bestemte regler for håndtering av helseopplysninger.[707] I undersøkelsen svarte primærleger på et spørreskjema, de aktuelle rettsreglene dreide seg i stor grad om samtykkekompetanse. Ut fra beskrivelsen i artikkelen synes spørsmålene om samtykkekompetanse både å være mer følsomme og noe mer kompliserte i Minnesota enn i norsk rett. Det kan henge sammen med et forhold som også påpekes i artikkelen, at samtykkekompetanse for mindreårige ofte anses som et inngrep i familienes rett til å styre oppdragelsen og beslutninger om egne barn. Spørsmålene til primærlegene gjaldt reguleringen av når mindreårige selv kan gi et gyldig samtykke, hva de kan samtykke til, og hva som krever foresattes samtykke. I undersøkelsen ble primærlegene bedt om å svare på om seksten forskjellige utsagn om samtykkekompetanse for mindreårige var riktig etter loven eller ikke. I tillegg skulle de svare på om hvert utsagn etter deres mening var, eller ville være, en god eller dårlig rettsregel. Resultatene, slik de er tolket i artikkelen, er at Minnesotas primærleger er relativt lite kjent med rettsreglene om mindreåriges samtykkekompetanse. Kunnskapene var noe bedre på områdene graviditet, prevensjon og øyeblikkelig hjelp enn på andre områder som rustiltak, psykiatri og innsynsrettigheter. Et annet interessant funn var at legenes holdninger til lovene, altså om den enkelte regel var god eller dårlig, viste at de var mer negative til at mindreårige selv kan be om innsyn uten foreldres samtykke enn til at mindreårige kan få helsehjelp uten foreldrenes samtykke.

7.2.2 Helsepersonells opplevelse av at taushetsplikten uthules

Uttrykket «uthuling av taushetsplikten» peker på en opplevelse blant helsepersonell, av at behandling av helseopplysninger er gjenstand for motsetningsfylte plikter.[708] En slik uthuling kan kanskje til en viss grad kvantifiseres gjennom utviklingen i antallet plikter til å rapportere ulike situasjoner. En slik kvantifisering vil likevel ikke gi noe helt dekkende bilde, blant annet har det stor praktisk betydning hvordan opplysningene brukes og beskyttes videre hos mottakeren. Uttrykket uthuling peker kanskje i vel så stor grad på en bekymring om økende krysspress mellom ulike forventninger om hvordan helseopplysninger skal håndteres. En gjennomgang av sakene i Rådet for legeetikk gjennom seksten år viser at helsepersonell har opplevd pliktene som gjelder håndtering av helseopplysninger som motsetningsfylte:

[707] Ellen M. Rock og Patricia S. Simmons (2003): «Physician knowledge and attitudes of Minnesota laws concerning adolescent health care». I: *Journal of pediatric and adolescent gynecology,* s. 101–108.
[708] Et eksempel, i tillegg til det som er sitert nedenfor, er høringsuttalelse fra Legeforeningen om forslag til nytt unntak fra taushetsplikt for kvalitetssikring, Prop. 23 L (2009–2010), s. 33.

> Et tilbakevendende spørsmål har vært uthuling av taushetsplikten når denne kommer i konflikt med samfunnshensyn, slik som utlevering av pasientlister til politiet for etterforskning av kriminalitet.[709]

Et annet eksempel på en situasjon der leger i konkret forstand har oppfattet taushetsplikten og andre hensyn som motsetningsfylte er i «Inkluderende arbeidsliv»-prosjektet. Selv om den personen som både er pasient og arbeidstaker i disse samhandlingssituasjonene i utgangspunktet samtykker til at opplysninger behandles, har involverte leger opplevd usikkerhet om hva de kan drøfte med en arbeidsgiver. Dette kommer blant annet frem i et forskningsnotat fra et følgeforskningsprosjekt:

> Spørsmålet om legens taushetsplikt overfor arbeidsgiver har stått sentralt i alle samlingene. IA-prosjektets oppfordring om dialog på arbeidsplassen og legenes oppgaver som bistandsaktør har skapt usikkerhet om hvorvidt legene selv må snakke med arbeidsgiveren om pasientens funksjonsevne. Dette vil i så fall lett kunne komme i konflikt med legens taushetsplikt og rolle som pasientens beskytter. Mange var usikre på hvor smart det var å snakke direkte med arbeidsgiver. Det kunne fort bli vanskelig å snakke om arbeidsfunksjon uten å komme inn på diagnose.[710]

Helsepersonells holdninger til taushetsplikt har også vært undersøkt empirisk. I en hovedoppgave i sykepleievitenskap ble det gjennomført en liten undersøkelse, der 20 sykepleiere ble spurt om etterlevelse av taushetsplikten.[711] I denne undersøkelsen mente 55 prosent av de spurte at de alltid overholder taushetsplikten. Dermed var det også et relativt stort mindretall som brøt taushetsplikten i ulike situasjoner. De fleste brudd forekom sykepleiere imellom, blant annet for å bearbeide sykepleiernes egen opplevelse av møtene med pasienter.

7.2.3 En undersøkelse av helsepersonells håndtering av helseopplysninger

Jeg gjennomførte også en egen, kvantitativ undersøkelse av helsepersonells håndtering av helseopplysninger. Den besto av et spørreskjema ble sendt ut til 700 profesjonsutøvere, fordelt på tre av de den gang 28 definerte gruppene helsepersonell, høsten 2007.[712] Svarprosenten var 57,4. Fordelingen mellom de tre helsepersonellgruppene var 300 leger (hvorav 200 som arbeider i sykehus og 100 primærleger), 200 helsesekretærer og 200 radiografer.

[709] Reidun Førde og Åsmund Hodne (2004): «Rådet for legeetikk 1985 - 2001». I: *Tidsskrift for Den norske lægeforening,* s. 936–938.
[710] Leif E. Moland (2005): «Med legene på laget: Et fagutviklingsprogram for å utvikle legenes rolle i et inkluderende arbeidsliv».
[711] Kari Anne Wikse (1995): «Taushetsplikten - hva og hvordan: har sykepleiere nok faglig kunnskap til å ivareta tillit og respekt mellom pasient og sykepleier når edb-baserte pasientjournaler innføres? : en teoretisk studie»
[712] Helsepersonelloven § 48(1). Antallet definerte grupper er nå 29.

Hensikten med å velge disse tre profesjonene var å få svar fra grupper som er ulike, både med hensyn til type utdanning, arbeidsoppgaver og relasjon til pasientene. Spørsmålene i skjemaet refererte til konkrete bestemmelser i helsepersonelloven, pasientrettighetsloven, helseregisterloven og norm for informasjonssikkerhet i helsesektoren. Det ble spurt om respondenten hadde opplevd den situasjonen som var beskrevet i regelteksten og hvor lenge det var siden. Der det var relevant ble det også spurt om hva de hadde valgt å gjøre i slike situasjoner, om de hadde handlet i tråd med eller mot pasientens ønsker med videre.

Det er ikke særlig utbredt å undersøke etterlevelse og virkninger av rettsregler kvantitativt. Årsakene er åpenbare: Man kan ikke slutte fra respondentenes erfaringer, og beslutningene de faktisk traff, til kunnskap om hvorvidt hver enkelt beslutning var riktig. Lovgivning kan regulere situasjoner som forekommer ofte eller sjelden, og et spørsmål om utfallet av respondentenes skjønnsmessige beslutning i en gitt situasjon røper ikke om beslutningen har vært triviell eller komplisert. Undersøkelsen bidrar derfor ikke til en rettsdogmatisk forståelse av reglene om håndtering av pasientopplysninger.

Spørreskjemaet besto av til sammen 26 spørsmål om temaet håndtering av opplysninger, i tillegg til bakgrunnsvariabler og en separat seksjon med spørsmål om holdninger til e-helsescenarioer. De 26 spørsmålene belyser fem forskjellige forskningsspørsmål. Resultatene finnes i samlet form, med tabeller over svarfordelinger for de ulike forskningsspørsmålene, i en publisert artikkel.[713] De resultater og vurderinger som gjengis her er mindre detaljerte hovedpunkter, med særlig relevans for avhandlingen.

7.2.3.1 Forekomst av unntakssituasjoner

Det første forskningsspørsmålet var om enkelte av de sitasjonene der helsepersonelloven gjør unntak fra taushetsplikten forekommer hyppig eller sjelden. Samlet sett er det ganske vanlig at helsepersonell befinner seg i en situasjon der de kan, bør eller skal gjøre unntak fra taushetsplikten, 40,8 prosent av respondentene hadde opplevd minst en av de situasjonene som var omfattet av spørreskjemaet.

Blant de typene situasjoner det ble spurt etter, var om respondentene hadde gitt opplysninger til barneverntjenesten om mistanker om omsorgssvikt. Blant leger utenfor sykehus, var andelen høy, 59,2 prosent hadde rapportert om slike forhold. Den samlede andelen, blant alle

[713] Herbjørn Andresen og Olaf Gjerløw Aasland (2008): «Helsepersonells håndtering av pasientopplysninger». I: *Tidsskrift for Den norske legeforening,* s. 2823–2827. Legeforeningens forskningsinstitutt bisto med faglige råd, hjelp til utsending, og hjalp til med analysen av resultatene. Undersøkelsen ble utført med hjelp til uttrekk av anonyme respondenter fra Legeforeningens forskningsinstitutt, Norsk Helsesekretærforbund og Norsk Radiografforbund.

tre grupper av helsepersonell som hadde opplyst om omsorgssvikt, var 22 prosent. Andelen på 59,2 prosent blant primærleger er imidlertid neppe vesentlig høyere enn man kunne forvente. En dansk undersøkelse, om ansatte i skolens plikt til å melde omsorgssvikt og særskilte sosiale problemer til sosialetaten, viste at 52 prosent av de spurte hadde innberettet mistanke om omsorgssvikt.[714]

7.2.3.2 Utfallene av helsepersonells skjønnsmessige beslutninger

Det andre forskningsspørsmålet gjaldt tendenser i utfallene av helsepersonells skjønnsmessige beslutninger om å innvilge innsyn eller etterkomme ønsker om å få korrigert journalens innhold. I utgangspunktet skal pasientens ønske tas til følge, men en beslutning som strider mot pasientens ønsker kan også, i spesielle situasjoner, være den mest riktige vurderingen.

Det er svært vanlig at helsepersonell opplever at pasienter gjør bruk av rettigheter til å påvirke håndteringen av opplysninger. 63,8 prosent av respondentene har svart bekreftende på at de har vært i minst én av de fem situasjonene i spørreskjemaet som gjelder pasienters aktive bruk av sine rettigheter. Av disse fem situasjonene var begjæring om innsyn i journal det mest utbredte. Til sammenligning viste befolkningsundersøkelsen om holdning til og kunnskap om personvern at bare 16 prosent av befolkningen har bedt om innsyn i opplysninger, uansett sektor, i medhold av personopplysningslovgivningen.[715]

I det samlede resultatet for alle de spørsmålene som kartlegger utfallet av respondentenes skjønn, er det en klar overvekt av beslutninger som er i overensstemmelse med pasientens ønske. Blant leger har 83,3 prosent av leger i sykehus og 84,2 prosent av leger i annen virksomhet vært i situasjoner der de har etterkommet pasienters ønsker om håndtering av opplysninger. Andelen leger som har vært i situasjoner der de etter en skjønnsmessig vurdering ikke har etterkommet pasientens ønske, er 6,5 prosent leger i sykehus og 10,5 prosent leger i annen virksomhet.

7.2.3.3 Etterlevelse av regler og retningslinjer

Det tredje forskningsspørsmålet var om regler og retningslinjer etterleves eller brytes. Svarene viste at to kategorier av regelbrudd var relativt hyppige. Den ene er det som kalles «snoking», altså urettmessig tilegnelse av opplysninger uten at opplysningene nødvendigvis bringes

[714] Sven Scharling m. fl. (2007): «Undersøgelse om forholdet mellem tavshedspligt og indberetningspligt». Undersøkelsen er gjennomført av et privat forskningsbyrå, på oppdrag fra en fagforening for undervisningspersonale. Materialet har vært brukt i en serie artikler i deres fagblad Månedsmagasinet Undervisere.
[715] Ravlum, s. 10.

videre til andre. Til sammen 17,6 prosent av respondentene hadde gjort dette minst én gang, hele 3,5 prosent av respondentene hadde «snoket» i løpet av de siste to ukene. Tallet er høyt nok til å indikere at dette foregår til daglig i helsetjenesten.

Den andre store kategorien av regelbrudd gjaldt også helsepersonells bruk av IT-systemer, men det dreide seg om et etterlevelsesproblem som nærmest er det motsatte av «snoking». Til sammen 5,1 prosent av alle respondentene, minst én gang latt være å lese opplysninger som de selv mener de *burde ha lest*, fordi de har vært hemmet av tanken på at IT-bruken kanskje kan spores gjennom logging. Tallene for øvrige regelbrudd i denne undersøkelsen var vesentlig lavere.

Et spesielt interessant aspekt ved etterlevelsen, for denne avhandlingens vedkommende, er eventuelle forskjeller mellom etterlevelsen av de pliktene som loven plasserer direkte på den enkelte profesjonsutøver, og etterlevelsen de plikter som følger av de reglene som virksomheten pålegger de ansatte å følge i medhold av de generelle sikkerhetsbestemmelsene. Konklusjonen på dette spørsmålet, den gang undersøkelsen ble gjennomført, var at det fantes et gap mellom hvor godt og forsvarlig pasientopplysninger håndteres, avhengig av hvor de aktuelle reguleringene hører hjemme. «Tradisjonelle» profesjonsbestemte plikter, og konkret utformete pasientrettigheter, overholdes og respekteres i stor grad. Det forekommer oftere brudd på de plikter som er nedfelt i systemer, rutiner og retningslinjer som helsepersonell skal overholde i egenskap av ansatte i en virksomhet som skal ivareta disse hensynene. Det kan synes som helsepersonell er mindre lojale til virksomhetsinterne retningslinjer enn til profesjonens internaliserte normer. Bakgrunnen for konklusjonen den gang var imidlertid at det såkalte snokeforbudet, rettet mot helsepersonell i lovs form, ikke var vedtatt på det tidspunkt undersøkelsen ble gjennomført.[716] En plikt til ikke å lete etter opplysninger man ikke har tjenestelig behov for ble derfor ansett som brudd på virksomhetens interne regelverk på det tidspunkt helsepersonellet besvarte spørreskjemaet. Denne delen av belegget for at direkte lovpålagte plikter for helsepersonell etterleves i større grad enn virksomhetenes interne regelverk, basert på lovpålagte plikter for virksomheten, vil ikke lenger kunne etterprøves på samme vis fordi selve snokeforbudet har «skiftet side».

7.2.3.4 Opplevelsen av tilgangskriterienes treffsikkerhet

Et fjerde forskningsspørsmål var hvordan helsepersonellet opplevde tilgangskriterienes treffsikkerhet. Dette forskningsspørsmålet er det som ligger nærmest avhandlingens problemstil-

[716] Helsepersonelloven § 21a og helseregisterloven § 13a, jf. nærmere omtale i kapittel 6.3.1.3 ovenfor.

ling, hvorvidt helsepersonell har tilganger som er tilstrekkelige, men heller ikke videre enn det som er tilstrekkelig, for å utføre pålagte oppgaver. Det man kan fange opp om treffsikkerheten, ved å stille spørsmål til helsepersonell på denne måten, er primært om tilgangene er for snevre. 26,5 prosent av respondentene har opplevd så sterke begrensninger i tilgangen til opplysninger at det har vært et reelt hinder i arbeidet. Halvparten av disse har opplevd så sterke begrensninger i løpet av de siste to måneder.

Hvorvidt tilgangene eventuelt skulle være unødvendig vide, kan respondentene egentlig vanskelig ta stilling til, med mindre de har utført vellykkede forsøk på å bryte reglene. Denne typen undersøkelse kan derfor bare gi indirekte indikasjoner på for vide tilganger, gjennom tallene for regelbrudd og gjennom svarene på hvorvidt adferden påvirkes av at virksomheten kontrollerer, eller kan kontrollere, hvordan tilgangene brukes.

7.2.3.5 Kontrollaktiviteters virkning på helsepersonells adferd

Det femte forskningsspørsmålet var om helsepersonells håndtering av pasientopplysninger blir påvirket av at virksomheten kan overvåke om IT-bruken er i tråd med retningslinjene, og om handlingene eventuelt påvirkes av en opplevd oppdagelsesrisiko. Spørsmålene var rettet til helsepersonell og gjaldt deres adferd. Hvorvidt overvåkning og detektering av brudd faktisk foregår i den enkelte virksomhet, og om tiltakene er effektive, har i prinsippet liten betydning for dette spørsmålet. I undersøkelsen ble helsepersonellet blant annet spurt om de hadde opplevd at virksomheten de arbeider i hadde konfrontert dem med mistanker om snoking. Det var en svært lav andel av respondentene som hadde opplevd at virksomheten har stilt spørsmål om hvilke grunner de har hatt for å lese eller håndtere helseopplysninger om en bestemt pasient. Fire respondenter hadde opplevd å bli konfrontert av sikkerhetsansvarlig, IT-ansvarlig, personvernombud eller tilsvarende funksjon i virksomheten med spesielt ansvar for håndtering av opplysninger. Kun én respondent hadde opplevd slik konfrontasjon fra en overordnet med personalansvar.

Selv om få har opplevd å bli konfrontert med mistanke om at opplysninger er lest eller håndtert urettmessig, er det ikke helt uvanlig at tanken på en mulig etterhåndskontroll fører til selvsensur. 15,6 prosent har unnlatt å lese opplysninger fordi de har vært engstelige for, eller mislikt tanken på, at handlingen kanskje logges. Som oftest har selvsensuren «riktig retning», 76,7 prosent blant de som var bekymret for loggingen har unnlatt å lese opplysninger som de uansett ikke hadde konkret behov for tilgang til. Imidlertid har også 35,9 prosent av den samme gruppen på 15,6 prosent unnlatt å lese opplysninger som selv mente at de burde ha

lest. 35,9 prosent av denne gruppen tilsvarer 5,1 prosent av alle de spurte. Virksomhetens kontroll med ansatte kan altså også ha utilsiktede virkninger.

7.3 Virksomheters kontroll med helseopplysninger

Fra et teoretisk og regulatorisk perspektiv kan man se det slik at omverdenens kontroll med hvordan en virksomhet håndterer helseopplysninger, og virksomheters egen kontroll med de ansattes bruk og eventuelle misbruk av informasjonssystemet, er to sider av samme sak. En virksomhets skal etablere og vedlikeholde planlagte og systematiske tiltak for informasjonssikkerhet.[717] Et eksternt tilsynsorgan fører tilsyn med at virksomhetens tiltak er på plass og fungerer.[718] Tilsynsorganets praksis er rettet inn mot å overvåke og beskrive avvik fra en angitt normativ tilstand, og eventuelt iverksette sanksjoner i den grad det både er grunnlag for det og det anses som hensiktsmessig. Virksomhetens kontroll med at helseopplysninger brukes på måter som er berettiget, og av ansatte som har fullmakt til og behov for det, er i praksis valg, iverksetting og håndheving av ulike tiltak som virksomheten selv vurderer som de best egnede for å innfri samme normative tilstand.[719]

7.3.1 Eksterne tilsyn som kilde til kunnskap om praksis

I hovedsak er det Datatilsynet som er relevant tilsynsorgan for informasjonssikkerhetsbestemmelser etter helseregisterloven. Helsetilsynet har imidlertid også et tilsynsansvar, som blant annet omfatter kontroll med at virksomheter sørger for at journal- og informasjonssystemene er forsvarlige.[720] Datatilsynet og Helsetilsynet har til og med gjennomført enkelte felles tilsyn, for å vurdere i sammenheng hvordan taushetspliktbestemmelser blir ivaretatt gjennom virksomhetens bruk av og tiltak for å sikre omfattende informasjonssystemer.[721] Tilsynsorganene kommuniserer sine funn og vurderinger både gjennom rapportene fra tilsyn med den enkelte virksomhet, og i form av årsmeldinger og andre sammenstilte eller aggregerte

[717] Helseregisterloven § 16.
[718] Jf. metodikken som er beskrevet ovenfor i kapittel 4, risikobasert internkontroll som reguleringsmetode.
[719] Skillet mellom en normativ tilsand som uttrykk for et ytre samfunnshensyn, og virksomhetens aktiviteter som operasjonalisering av den normative tilstanden, er hentet fra betraktningene om virksomheters handlingsrom som teknologisk representasjonsproblem, jf. kapittel 2.2.3.
[720] spesialisthelsetjenesteloven § 3-2 jf. helseregisterloven § 31.
[721] Jf. *Rapport frå tilsyn med informasjonstryggleiken ved pasientjournalsystemet Doculive og det pasientadministrative systemet PIMS ved Helse Bergen HF, Haukeland universitetssjukehus* (2006), og *Rapport fra tilsyn med konfidensialiteten og tilgjengeligheten til elektronisk pasientjournal ved Akershus universitetssykehus HF* (2006).

vurderinger. Et eksempel på sammenstilte vurderinger, som kanskje er noe polemisk i formen, er en rapport fra Datatilsynet, utgitt som debattinnlegg i en lovendringssak kort tid etter at den hadde vært på høring.[722] Helsetilsynet gjør også rede for en sammenstilling av erfaringer fra sine tilsyn om disse temaene i et brev til Helse- og omsorgsdepartementet.[723]

Summen av tilsynsorganenes vurderinger er på sett og vis dyster lesning, som tegner et generelt bilde av at virksomhetenes tiltak og aktiviteter ikke er tilstrekkelige for å ivareta informasjonssikkerheten generelt, og konfidensialitetsvernet spesielt. I utgangspunktet er disse vurderingene troverdige, og de beskriver reelle problemer i virksomhetenes praksis. Tilsynsorganenes vurderinger er basert på fagmessig utført systemrevisjon, dokumentasjon av de enkelte funn, tilsvarsmuligheter for tilsynsobjektet, og åpenhet om resultatene.

Likevel er det behov for noen betraktninger om tilsynsorganenes meddelelser til verden, både i lys av deres samfunnsoppdrag og i lys av visse trekk ved internkontroll som reguleringsmetode, uten at det dermed settes spørsmålstegn ved om funnene stemmer. Tilsyn er i seg selv ofte en jakt på svakheter, og for et så komplisert fag som informasjonssikkerhet, som naturlig nok skal ha begrensede ressurser i en virksomhet som ikke har dette som hovedoppgave, bør det i seg selv ikke være overraskende at svakheter finnes.

Et første tankekors er at beskrivelser av grove avvik, til dels i svært stort omfang, ofte møtes med relativt milde sanksjonstrusler og lite konkretiserte utbedringskrav. Lite konkretisering av hva slags tiltak som forventes for å utbedre et problem kan skyldes respekt for virksomhetens handlingsrom, og hensynet til fleksibilitet og kontinuitet. Det er en tolkning som er i tråd med internkontrollideologien, et problem bør håndteres i den virksomheten der problemet oppstår. En alternativ tolkning er at tilsynsorganet velger virkemidlene strategisk, slik at både valg av hvor alvorlig avvikene fremstilles og valg av sanksjonsmidler har samfunnet utenfor virksomheten som adressat. Det vil si at oppmerksomhet om forholdene og allmennpreventive hensyn kanskje vektlegges mer enn hvilke forbedringer som oppnås i den enkelte virksomhet.[724] I et slikt perspektiv vil et tilsynsorgans arbeid for å sikre eget omdømme og faglige anerkjennelse kunne ha betydning for beskrivelsene av både problem og avhjelpning.

---

[722] *Sviktende tilgangsstyring i elektroniske pasientjournaler? Lovforslag om å tillate direkte tilgang til pasientjournaler på tvers av virksomhetsgrensene* (2009). Rapporten var foranlediget av høringsutkastet til det som senere ble endringslov 19. juni 2009 nr. 68, som det er mange henvisninger til i kapittel 5 ovenfor.

[723] Helsetilsynet, «Mangelfull tilgangsstyring til elektronisk pasientjournal truer taushetsplikten i sykehus (Brev til Helse- og omsorgsdepartementet)»: *http://www.helsetilsynet.no/templates/LetterWithLinks____9430.aspx*.

[724] For en mer omfattende drøfting av strategiske valg av virkemidler, se Tommy Tranvik (2009): *Personvern og informasjonssikkerhet. En studie av rettsreglers etterlevelse i kommunal sektor*, s. 98–103.

En annen betraktning, om eksterne tilsyn som kilde til kunnskap om praksis, gjelder selve utformingen og underbyggingen av avviksbeskrivelser. Det følgende eksemplet er den første av to avviksformuleringer i Datatilsynets og Helsetilsynets felles tilsyn ved Ahus i 2006. Det egner seg som eksempel her, fordi det omhandler en praksis av det slaget som motiverer avhandlingens problemstilling.

> Avvik 1: Akershus universitetssykehus HF sikrer ikke at taushetsbelagte personopplysninger i det elektroniske pasientjournalsystemet DIPS er forsvarlig vernet mot innsyn fra ansatte som ikke har legitimt behov for opplysningene.
>
> Avvik fra: Pasientjournalforskriften § 4 bokstav f, jf spesialisthelsetjenesteloven § 3-2 første ledd, jf internkontrollforskriften § 4, jf helseregisterloven §§ 13 og 16, jf § 36, jf personopplysningsforskriften § 2-14.[725]

Denne avviksformuleringen er underbygget med 19 etterfølgende punkter, eller funn, fra de ulike leddende i systemrevisjonen. Det første funnet er at virksomhetens besluttede tilgangspolitikk er at tilgangene skal være vide, for å unngå omfattende bruk av ad hoc selvautorisering. Dette funnet kunne ha vært løftet frem som selvstendig avvik, og for den saks skyld ha vært gjenstand for direkte overprøving. En overprøving ville imidlertid innebære at tilsynsorganene tok stilling til hvorvidt ad hoc selvautorisering er et bedre tiltak enn vide tilganger. Det er for det første et relativt stort inngrep i virksomhetens handlingsrom, og dernest vanskelig å forsvare som en generell informasjonssikkerhetsfaglig vurdering. Dermed blir dette funnet stående som et relativt svakt funn i seg selv, en vurdering som det kan stilles spørsmål ved. Ut fra en internkontrolltankegang ville fravær av en tilgangspolitikk være alvorlig, mens en diskutabel tilgangspolitikk er, vel, diskutabel.

De fleste av de etterfølgende punktene beskriver hva ulike grupper helsepersonell faktisk har tilgang til, og underbygger med det at tilgangene er vide. Avviksbeskrivelsen henviser til helseregisterloven § 13, dermed impliseres at de vide tilgangene strider mot kravet om at tilganger bare kan gis i samsvar med gjeldende bestemmelser om taushetsplikt. Det påpekes også at ikke alle mulighetene programvaren gir for å snevre inn tilgangene er brukt. Det er imidlertid ikke nærmere begrunnet eller sannsynliggjort at bruk av alle programvarens muligheter ville ha truffet behovet bedre. Videre peker to av funnene på at de vide tilgangene påvirker innholdet i journalen, altså hva man velger å dokumentere eller å la være å dokumentere. De fem siste funnene dreier seg om ulike mangler ved rutiner, metoder og verktøy for å avdekke urettmessig tilgang gjennom etterhåndskontroller.

[725] *Rapport fra tilsyn med konfidensialiteten og tilgjengeligheten til elektronisk pasientjournal ved Akershus universitetssykehus HF*, s. 5.

Til sammen underbygger funnene avviksbeskrivelsen godt, først og fremst ved å dokumentere et stort volum av forhold som sannsynliggjør at kontrollen er svak og at overtramp kan bli vanskelige å avdekke. Faktiske forekomster av misbruk er, i tråd med det som er vanlig for systemrevisjoner, ikke tema i rapporten. Virksomhetens tilsvarsmuligheter gir også en grei kvalitetssikring av funnene.

Det som imidlertid kan være noe mer problematisk med denne måten å underbygge avviket på, er at det skapes et inntrykk av at visse bestemte tiltak vil kunne avhjelpe de ulike funnene. Blant de tiltakene som ikke pålegges direkte, men som det gis inntrykk av at vil følge «logisk» fra funnene, er en ny og strammere tilgangspolitikk, mer omfattende bruk av programvarens muligheter for å snevre inn tilgangene, og bruk av logganalyseverktøy for å avdekke uberettiget tilgang. Det kan være riktig, delvis riktig, riktig under visse forutsetninger, eller riktig men langt fra det mest effektive tiltaket for å avhjelpe funnene. Med bakgrunn i denne avhandlingens påstander om sammenhengene mellom ulike metodetrinn i internkontroll som reguleringsmetode, er det sterkeste argumentet for at en virksomhet selv bør ha størst mulig kontroll med beslutninger om tiltakene nettopp at det ikke er en sterk logisk forbindelse mellom risikofaktorer, risikoreduserende tiltak og avvik.[726] Med andre ord, tilsynsrapporter gir bred og generelt troverdig kunnskap om praksis, men det vil være mer tvilsomt å lese slike rapporter som et belegg for slutninger av typen «dersom *tiltak T* hadde vært iverksatt, ville *avvik A* ha vært unngått».

7.3.2 Praktisering av kontroll i virksomhetene

For å bygge ut og nyansere kunnskapen om praksis i virksomhetene har det vært behov for å supplere den kunnskapen man får fra å lese rapporter fra tilsynsorganenes systemrevisjoner. Her presenteres noen resultater fra mine egne kvalitative undersøkelser. Disse undersøkelsene omfatter bare spesialisthelsetjenesten, og dekker derfor bare en relativt begrenset del av avhandlingens område. Spesialisthelsetjenesten består imidlertid av store og kompliserte virksomheter, så de gir muligheter for et godt innblikk i en del sider ved sikkerhetsarbeidet. Det er likevel ikke usannsynlig at man ville få et annet bilde av praksis ved å undersøke en sentral registervirksomhet, for eksempel Helfo eller Folkehelseinstituttet. Etter hvert vil det også være av stor interesse å undersøke hvordan helseopplysninger håndteres mellom en databehandlingsansvarlig og andre involverte virksomheter i virksomhetsovergripende, behandlingsrettede helseregistre, men det er det foreløpig for tidlig å undersøke som praksis.

[726] Jf. kapittel 4.3.3–4.3.6 ovenfor.

Hoveddelen av undersøkelsen er fire intervjuer, gjennomført ved to forskjellige enheter i samme helseforetak. For å oppnå en viss bredde i perspektivene er det valgt intervjuobjekter med ulike oppgaver i virksomheten, en sikkerhetsleder, en operativ systemeier, altså en person som har fått systemeieroppgaver delegert fra helsefaglig direktør, en avdelingsoverlege og en tillitsvalgt med underordnet stilling som helsepersonell. I tillegg er en del informasjon, om diskusjoner rundt internt besluttede tilgangskriterier, innhentet gjennom deltakelse på seminar og uformelle samtaler med ulike aktører ved et annet helseforetak, i en annen helseregion. De kvalitative dataene er innsamlet i perioden oktober og november 2009.

I intervjuene var utgangspunktet at de samme spørsmålene ble stilt til alle intervju-objektene. Spørsmålene dreide seg om ulike sider ved praktisering av og erfaring med det å avdekke urettmessig tilgang til helseopplysninger blant virksomhetens ansatte. Hvert intervju var av 50–70 minutters varighet, og tok utgangspunkt i en intervjuguide med åpne svaralter-nativer. Spørsmålene hadde stort sett formen «hvordan foregår …?» gjerne fulgt opp med spørsmålet «hva står det der?» når det henvises til skriftlige rutiner eller innhold i en logg eller et IT-system. Ved et par anledninger kjente ikke intervjuobjektet til konkrete erfaringer med den typen hendelse spørsmålet gjaldt, i slike situasjoner ble spørsmålet omformulert til å gjelde en antakelse om hvordan en hypotetisk situasjon ville ha blitt håndtert. Samtalene tok litt ulike retninger med de forskjellige intervjuobjektene, men det bildet som ble gitt av praksis var i det store og hele sammenfallende. Det viktigste funnet var kanskje likevel ikke svarene på de enkelte spørsmålene, men et helhetsinntrykk som ble forsterket fra intervju til intervju: Det utøves et ganske betydelig, jevnt og systematisk sikkerhetsarbeid, det har legitimitet i virksomheten selv om det er ulike oppfatninger om enkelte ting, og man har god kjennskap til styrker og svakheter i dette arbeidet.

7.3.2.1 Tilgangskriterier

Sikkerhetsleder og systemeier forholder seg først og fremst til tilgangskriteriene som noe virksomheten beslutter, og som iverksettes så godt det lar seg gjøre i virksomheten. Et samsvar med gjeldende bestemmelser om taushetsplikt etterstrebes, men IT-systemene har sine muligheter og begrensninger. Det overordnede tilgangskriteriet for EPJ-systemet er rolle-basert tilgang, først og fremst med en faglig rolle, ut fra hvilken gruppe helsepersonell databrukeren tilhører. Rollene er videre delt inn i nedslagsfelt, etter databrukerens organisa-toriske plassering. Den faglige rollen avgrenser hvilke typer informasjon man får tilgang til i EPJ-systemet.

For enkelte typer særskilt sensitive opplysninger er det bare individuelle brukere, eller helt smale roller, som gis tilgang. En del av fagsystemene har mindre utbygd tilgangskontroll, men da er det også færre yrkesgrupper som er definert som brukere, det kan for eksempel være fagsystem som bare brukes av bioingeniører.

En konkret regel om tilganger, som flere helseforetak har nedfelt i sine kriterier, er et forbud mot å se på sin egen journal. Dersom man sammenholder dette med helseregisterlovens generelle bestemmelse om tilganger, er dette i tråd med første del av setningen: «Tilgang kan bare gis i den grad dette er nødvendig for vedkommendes arbeid», mens det å se på sin egen journal i utgangspunktet ikke ville være i strid med gjeldende bestemmelser om taushetsplikt.[727] Bakgrunnen for at dette er nedfelt i tilgangskriteriene er altså først og fremst at å lese sin egen journal ikke er definert som et tjenestelig behov.

Dette kriteriet har, flere steder, blitt møtt med manglende forståelse og til og med motstand fra helsepersonell. For personer som arbeider med sikkerhet, og skal utforme tilgangskriterier etter gjeldende føringer, virker et slikt kriterium nærliggende og nærmest selvfølgelig. Helsepersonell, som først og fremst har et faglig og praktisk forhold til journalen, er tilbøyelige til å oppfatte et slikt kriterium som unødvendig, rigid, eller til og med krenkende.

Et annet kriterium, som er vedtatt i virksomheten og som helsepersonell har vist liten forståelse for, er at den legen som selv har henvist en pasient til en annen avdeling ikke har anledning til å se denne pasientens journal i ettertid. Legen som har henvist anser det for å være et tjenestelig behov for å se hvordan det gikk videre med pasienten, og gjerne lære noe av det videre forløpet. Virksomhetens syn er imidlertid at det ikke er et tjenestelig behov fordi legens egen læring ikke i tilstrekkelig direkte forstand er å yte helsehjelp til pasienten.

7.3.2.2 Medbestemmelse

Spørsmål om innsyn, eller om å få slettet opplysninger fra journalen, er forhold som er relativt vanlige og som følger greie rutiner. Utgangspunktet er en forespørsel fra pasienten. Dersom den legen som har dokumentert opplysningene er enig, blir innsyn gitt eller opplysningene slettet. Dersom legen ikke er enig, og pasienten fremdeles står på sitt ønske går saken oppover i linja. Ved fortsatt uenighet i slike spørsmål forekommer det også at pasienten går videre, og bruker pasientklagekanalene, i praksis vil det si ombud eller tilsyn.

[727] Jf. helseregisterloven § 13(1) annet punktum. Generelt er taushetsplikt ikke til hinder for at opplysninger gjøres kjent for den opplysningene direkte gjelder, jf. helsepersonelloven § 22. Det kan likevel være grunner til at den som har dokumentert opplysningene bør involveres i en vurdering, for eksempel for å ta stilling til om innsyn er utilrådelig av hensyn til personer som står pasienten nær, jf. pasientrettighetsloven § 5-1.

Pasienters ønsker om å sperre journal var det noe større usikkerhet om blant intervju-objektene. Alle var kjent med at slike rettigheter finnes, men ikke like sikre på rutinen og på hva som er teknisk gjennomførbart. I følge sikkerhetsleder har imidlertid helseforetaket gode rutiner for dette. Dersom en pasient melder et ønske om å sperre en journal, er det et skjema for dette som fylles ut sammen med behandler. Ofte er det et poeng å unngå at pasienten sperrer så mye av opplysningene at det blir vanskelig å behandle vedkommende. I praksis dreier gjennomgangen sammen med behandler seg om å gå gjennom hvilke opplysninger man ønsker sperret, og så samle dette i ett, eller noen få, journalnotater som sperres. Det har vært noen interne meningsforskjeller om hvordan og i hvor stor grad pasientene skal informeres om adgangen til å sperre opplysninger. Slik informasjon finnes i et lite avsnitt i en brosjyre som deles ut til pasientene.

Avdelingsoverlegen som ble intervjuet syntes ikke å være kjent med det aktuelle skjema, og sa at han selv ikke vet helt hva som er mulig eller ikke mulig av sperring. Likevel traff han så nær sikkerhetsleders beskrivelse på et «hva ville du ha gjort»-spørsmål at det er grunn til å regne med at det ville ha ordnet seg i praksis: Han ville først ha tatt en samtale med pasienten, om hva som ønskes sperret, og deretter tatt dette videre til administrasjons- og IT-miljøet for å få det iverksatt.

7.3.2.3 Etterhåndskontroll av tilganger

Den viktigste motivasjonen for å gjennomføre intervjuer i et helseforetak var et behov for mer håndfast kunnskap om etterhåndskontroll av at tilgangskriterier er overholdt. Politiske initiativer, der det tas til orde for mer omfattende behandling av helseopplysninger, både forutsetter at denne typen tiltak er etablert og fremholder det som en type tiltak som vil øke vesentlig i utbredelse og effektivitet nær fremtid.[728]

Etterhåndskontrollen gjennomføres ved å undersøke ulike typer elektroniske spor, som kan vise hvilke ansatte som har sett, sendt eller endret opplysninger. Den alminnelige samle-betegnelsen for ulike varianter av slike spor er «logger». En logg er i de fleste tilfeller en sekvensiell fil utenfor den strukturerte databasen med helseopplysninger, der data om hvilke handlinger en pålogget bruker utfører blir føyd til fortløpende. Logging av dette slaget er en aktivitet i systemet som databrukeren normalt ikke legger merke til, og ikke trenger forholde seg til. I en del tilfeller genererer samme IT-system flere ulike logger, til ulike formål. Enkelte typer sporingsinformasjon, som man ønsker at skal være enklest mulig tilgjengelig, kan også

[728] Se for eksempel Ot.prp. nr. 49 (2005-2006) s. 27, Ot.prp. nr. 51 (2008-2009) s. 24 og Prop L. 23 (2009-2010) s. 22.

integreres i den strukturerte databasen, for eksempel slik at en liste over hvem som har sett på journalen til en gitt pasient kan hentes direkte ut fra journalsystemet uten å gå veien om eksterne logger.

I det aktuelle helseforetaket dannes loggene primært fra journalsystemet (EPJ), og fra et pasientadministrativt system (PAS) som blant annet brukes til sykepleiedokumentasjon. De kliniske fagsystemene genererer ikke logger, det gjør heller ikke laboratoriesvar- og røntgenbildesystemene. En del saksbehandling foregår i et eget arkivsystem, blant annet gjelder det forsendelser av opplysninger til barnevern, og en del klagesaksbehandling. Oppslag i disse opplysningene logges heller ikke. Det har vært noe diskusjon ved helseforetaket om hvorvidt en del av disse opplysningene egentlig heller burde ligge i pasientjournalen.

EPJ-systemet genererer forskjellige logger. Den ene er en «innsynslogg», som er en del av EPJ-produktet, der loggopplysninger som identifiserer både databrukeren og pasienten blir lagt automatisk ut på egen fil. EPJ-systemet genererer også en mer omfattende systemlogg, som kan gi mer informasjon men som det også er vanskeligere å analysere. Det er ikke alle typer oppslag i EPJ-systemet som logges, medikasjonsinformasjon og visse andre fellesbilder ligger i EPJ-systemet, og er knyttet til pasienten, men er likevel åpent tilgjengelig for påloggede brukere. En annen logg fra EPJ-systemet, den som brukes mest i praksis i arbeidet med etterkontroller, er den såkalte «blålysloggen». Den kontrolleres regelmessig. Avdelingsoverlegen som ble intervjuet har i praksis aldri sett andre logger enn den. Erfaringene med å kontrollere blålyslogger er også et tema i en årlig «ledelsens gjennomgang» av informasjonssikkerheten ved foretaket.[729]

Blålysloggen genererer en ny linje hver gang en ansatt bruker en blålystilgang, for ad hoc selvautorisering, dersom vedkommende har behov for tilgang uten å ha tilgang etter ordinære kriterier.[730] Ved bruk av blålystilgang angir databrukeren en fritekst begrunnelse for hvorfor tilgang er nødvendig. Denne begrunnelsen fremkommer i blålysloggen. Flere av intervjuobjektene anså bruken av fritekst som en kilde til lav kvalitet i begrunnelsene. Ofte blir det brukt vage, nærmest intetsigende formuleringer, for eksempel «helsehjelp til pasienten.» Det forekommer også mindre seriøse angivelser som «idiot» eller «qwert» (første tegnsekvens øverst til venstre på tastaturet). Under intervjuet viste avdelingsoverlegen frem et par ferske eksempler på utskrift av blålyslogg. En linje viste en ansatt som har vært inne på egen journal, og kun én gang. Den angitte begrunnelsen var «jeg ville teste om noen følger med på at jeg

[729] Ledelsens gjennomgang, som en regelmessig aktivitet, er et trinn i det forskriftsfestede, systematiske sikkerhetsarbeidet, jf. personopplysningsforskriften § 2-3.
[730] Dette er en variant av det mer generelle begrepet «nødrettstilganger» i Norm for informasjonssikkerhet i helsesektoren, jf. kapittel 6.4.2.4 ovenfor.

ser på min egen journal.» En annen bruker hadde flere linjer i loggen, der det ikke var skrevet ordentlige begrunnelser, bare trykket noen vilkårlige taster. Intervjuobjektet betraktet det som et uttrykk for den ansattes mening om kravet til å begrunne blålystilgang. Funnet av en uholdbar eller useriøs begrunnelse i loggen tas opp med vedkommende, som bes om å kommentere det som er angitt, hvorpå lederen forteller den ansatte hva som forventes.

I prinsippet skal all blålystilgang følges opp som avvik, men foreløpig anser de det som uoverkommelig å gjennomføre systematisk avviksbehandling fordi volumet av bruken er for stor. En reell etterprøving skjer stort sett bare i enkelte tilfeller der de har en konkret mistanke om misbruk, eller dersom en pasient ønsker å vite hvorfor en bestemt ansatt har sett på journalen.

Blålystilganger kan betegnes som en av flere mulige aktualiseringsmekanismer. Ulike EPJ-systemer i spesialisthelsetjenesten har av og til flere forskjellige slike mekanismer, med ulik terskel for når de kan brukes, og som de i ulik grad velger å følge opp konkret som avvik. Ved det aktuelle helseforetaket er blålystilganger foreløpig den eneste aktualiseringsmekanismen som brukes, men man er også i ferd med å ta i bruk en såkalt «grønnlystilgang», som er en annen mekanisme som tilbys i samme EPJ-produkt. Da velger databrukeren mellom faste, kodede begrunnelser, som gir tilgang innen visse rammer og oftest for en begrenset periode. Grønnlystilgangene havner også i en egen logg, skilt ut fra annen teknisk logging og fra blålyslogg. Grønnlystilganger følges ikke automatisk opp som avvik. Helseforetaket håper å få redusert omfanget av blålystilganger på denne måten, slik at blålys kan bli gjenstand for tettere oppfølging. På lenger sikt ønsker man også å legge om til mer dynamisk tilgangskontroll, basert på behandlingsforløp, som reduserer behovet for aktualisering ytterligere.

I PAS-systemet er en innsynslogg integrert i databasen, og følger automatisk med i den rapporten som leveres ut når en pasient ber om innsyn. Innsynsloggen fra PAS-systemet er likevel ikke helt pålitelig i så måte, fordi det hender at sykepleiere i løpet av en vakt skriver notatlinjer under en annen ansatts innloggete journalnotat, fordi ny pålogging kan være for tidkrevende. I slike tilfeller skriver man sine egne initialer ved siden av det man har skrevet inn i notatet, mens innsynsloggen peker på den påloggede sykepleieren. Kvalitetssikringen av dette ligger i at vaktleder godkjenner rapporten før den avsluttes ved vaktskifte.

De såkalte tekniske loggene, i praksis andre logger enn blålysloggen, er krevende å bruke systematisk til å avdekke misbruk. En analyse av logginformasjonen forutsetter ofte at flere innslag ses i sammenheng, og det er av og til også nødvendig å trekke inn flere andre informasjonskilder for å få kunnskap om hva som har foregått. Ved dette helseforetaket

begrenser slik gransking seg som oftest til å lese gjennom enkeltinnslagene, og spørre den det gjelder om forklaring. Sikkerhetslederen bruker, i beskjeden målestokk, et egenutviklet og enkelt verktøy for å bearbeide logginformasjon, men har ikke gode profesjonelle verktøy for dette. Sikkerhetsleder antar at bedre analyseverktøy vil kunne ha mye å si for nytten av logger. I den forbindelse omtaler han to prosjekter ved andre helseforetak, for å utvikle verktøy og metoder som kan brukes til å finne mistenkelige handlingsmønstre, og gi varsler om aktivitet i systemene som det kan være grunn til å undersøke nærmere. Disse prosjektene oppfattes imidlertid «å gå litt i rykk og napp», så det er usikkert hvor langt frem det ligger at de vil kunne nyttegjøre seg de nye og bedre metodene ved dette helseforetaket.

Ved dette helseforetaket er det lite ressursallokering til kontroll av logger, det er ikke en fast bemannet oppgave. I forbindelse med elektroniske meldingsutveksling er det et behov for å få på plass og bemanne det som kan kalles «operativ logging». Den elektroniske meldings-utvekslingen mellom helseforetaket og andre aktører forutsetter håndtering av kvitterings-meldinger, og retting og omsending ved feil eller når en melding ikke har kommet frem. At dette ikke er på plass er til noe frustrasjon for blant annet leger som henviser pasienter til helseforetaket. Ettersom den operative loggingen ikke er på plass, brukes papirdokumenter som sikkerhetskopi for å dokumentere handlinger i ettertid.

Det finnes rutiner ved helseforetaket for hvem som kan rekvirere analyse av logger. I praksis er det som oftest initiert av et ønske fra pasienten. Sikkerhetsleder anslår at det er tilfelle i mellom 80 og 90 prosent av tilfellene, men understreker at det ikke er basert på noen opptelling. Når en logganalyse er rekvirert, er det er sikkerhetsleder som går gjennom loggene og vurderer innholdet.

Ved mistanke sjekkes først innsynsloggen. Den databrukeren som eventuelt får mistanke rettet mot seg får anledning til å uttale seg. Dersom det er pasienten som har meldt mistanke, får også pasienten se loggen, og blir forklart hva oppslagene dreier seg om. Det er svært sjelden pasienten ønsker noen videre forfølging av saken etter det. I noen tilfeller er det sykehuset som har mistanke om misbruk av tilganger, da konfronteres vedkommende av overordnet med personalansvar. I slike situasjoner selekteres og sorteres handlinger knyttet til den aktuelle databrukeren. Den som er nærmeste overordnede til en som mistenkes tar saken videre, eventuelt som personalsak. Slike saker er svært sjeldne, det har ikke vært noen det siste året. Det utelukkes ikke at flere saker kunne ha kommet opp dersom logger ble analysert mer systematisk og med bedre verktøy.

Avdelingsoverlegen som ble intervjuet har to ganger opplevd at en pasient har meldt inn mistanke om snoking blant ansatte han er ansvarlig for. I begge disse tilfellene spurte han

pasienten om aktuelle tidspunkter med videre, og kontaktet sikkerhetsleder for å få en gjennomgang av logg for vedkommende ansatt i aktuelle tidsrom. Pasienten ble informert om hva som ble funnet, deretter ble den legen det gjaldt informert. I en av disse to situasjonene var det ut fra loggen liten grunn til å tro at noe var skjedd. I den andre situasjonen ble pasient og lege informert, men ingen større konfrontasjon av legen, eller sanksjoner i noen form, ble iverksatt.

Håndtering og undersøkelse av logger er, i hvert fall så langt, et rent internt anliggende i eget sikkerhetsarbeid. Det har ikke vært noen utveksling av logginformasjon, og det foregår ingen systematisk rapportering av funn til styrende myndigheter eller tilsynsorganer. Helseforetaket har ikke rutiner for å slette innsynslogg, og har heller ikke gjort det foreløpig. Når en pasient ønsker innsyn i loggen, ligger det ofte et stykke tilbake i tid.

Noe som kom frem gjennom intervjuene, uten at det sto på spørsmålsblokken, var at helseforetaket har definert noen fellesbrukere i Active Directory, med svært begrensede tilganger i nettet.[731] Når en slik fellesbruker er logget på, kan flere personer bruke EPJ og PAS fra samme datamaskin. Det gis imidlertid ikke tilgang til e-postsystemet eller personlige filområder ved fellespålogging. Hensikten er at det går vesentlig raskere å bytte bruker, fordi man slipper å logge seg helt ut av Windows-nettet først. Helseforetaket anser dette som forsvarlig fordi EPJ-systemet har egen brukerdatabase, og ikke kommuniserer med andre systemer under slik pålogging. Dette er en politikk som imidlertid vil måtte revurderes ved eventuell etablering av gjennomgående pålogging eller ved mer utstrakt integrasjon mellom EPJ og andre IT-systemer.[732] Når PAS-systemet brukes av sykepleiere på post, er også dette systemet svært ofte startet opp under fellesbruker, men med individuell pålogging til applikasjonen. Fellesbrukere er ikke anerkjent som et godt informasjonssikkerhetstiltak, det frarådes generelt i tekniske standarder for informasjonssikkerhet.[733]

I tillegg til spørsmålene om praksis, ble det også spurt om hvilke tanker de gjorde seg om ansattes opplevelse av og holdning til sporbarhet, og om hvorvidt de regner med at etterhåndskontroll av tilganger vil bli mer utbredt fremover. Generelt trodde ingen av intervjuobjektene at de ansatte hadde noen sterk, negativ opplevelse av at de ble overvåket av

[731] Windows Active Directory er systemmiljøets grunnleggende mekanisme for identifisering og autorisering av komponenter og brukere. Dersom det er behov for å sammenholde logger fra de ulike helsefaglige IT-systemene med logginformasjon fra det underliggende systemmiljøet, forutsetter det at den enkelte databruker er individuelt autentisert også i Active Directory.

[732] Gjennomgående pålogging oppnås ved å bruke samme kilde til informasjon om databrukerens identitet, og samme autentiseringsmekansisme, for flere IT-systemer. Det omtales ofte som «Single Sign-on», jf. Thale Omveien (2010): *Tribus Lingua – håndbok i teknokratsjargong*.

[733] Blant annet NS-ISO/IEC 17799:2005, s. 38. Det åpnes for at bruk av gruppe-identifikatorer kan tillates «der arbeidets art tilsier det», noe som kan være åpent for diskusjon i denne typen situasjoner.

arbeidsgiver. De mente blant annet at det å vite at handlinger blir fulgt opp kan være et «sunt filter» for å utvikle gode holdninger om at tilganger bare skal brukes ved faglige behov, at dette er noe ansatte vender seg til og bør tåle, og at det kommer til å bli et generasjonsskifte der yngre ansatte som er vokst opp med den nye teknologien ser på kontroll og sporbarhet som en helt naturlig del av arbeidssituasjonen. Loggingen anses å ha en positiv, pedagogisk side, «man skal vite at man blir kikket i kortene». I konkrete saker, der en ansatt blir utsatt for mistanke, antok et av intervjuobjektene at den ansatte kanskje i større grad ville få følelsen av å ha arbeidsgiver mot seg når mistanken er initiert av arbeidsgiver, enn om det er pasienten som har reist mistanken.

Ansattes personvern har i relativt liten utstrekning vært tema blant ansatte og fagforeningen, de har vært mer inne i bilde ved utarbeidelse av e-postpolitikk og lignende som ikke i samme grad har med pasientene å gjøre. Fagforeningsrepresentanten kunne fortelle at det pr. i dag ikke var rutiner som regulerte når, hvor og hvordan tillitsvalgte hadde blitt koblet inn i en konflikt som gjelder mistanke om snoking. Intervjuobjektet som selv var tillitsvalgt ville ha foretrukket å bli koblet inn i konkrete situasjoner, etter en hendelse, og ikke i utarbeiding av virksomhetens retningslinjer. Det ville likevel være ønskelig å kobles inn tidlig, før den konkrete hendelsen hadde tilspisset seg. Å bli koblet inn etter at en konflikt har tilspisset seg er ofte i seneste laget.

Alle som ble intervjuet var samstemte i vurderingen av at kontroll med logger for å avdekke misbruk av tilganger allerede var akseptert av de fleste, og at det ville bli mer av det fremover.

Del III:

Autorisasjonsprinsipper og kontrollteknologi

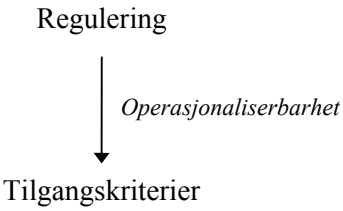
8 Analytisk ramme for egnethetsvurderinger

I denne siste delen av avhandlingen gjennomgås spørsmålet om hva slags prinsipper for teknologiske representasjoner, av regler om tilgang og videreformidling, som kan være egnet til å ivareta et samsvar mellom reguleringen og tilgangskriteriene. Et autorisasjonsprinsipp kan betraktes som en generell, men retningsgivende beskrivelse av hvordan tilgangskriterier skal kunne representeres i informasjonssystemer. I denne delen av avhandlingen er de ulike autorisasjonsprinsippene som vurderes og beskrives på et noe mer konkret nivå enn de overordnede prinsippene «need to know» eller «need to protect».[734] Nivået er mindre detaljert enn det man vanligvis finner i kravspesifikasjoner eller logisk design i et systemutviklingsprosjekt. Det er imidlertid sammenheng mellom nivåene: Som regel vil det være enkelt å se, i en konkret tilgangskontrollmekanisme, hvilket bakenforliggende autorisasjonsprinsipp den er basert på. En analogi som antyder hvilket abstraksjonsnivå denne typen autorisasjonsprinsipper befinner seg på, er valget mellom fartsdumper, fotobokser eller ferdsskriver i bilen som teknologiske prinsipper for å sikre at fartsbegrensninger overholdes i veitrafikken.

Om ikke det finnes ett enkelt autorisasjonsprinsipp som på en klar og overbevisende måte oppfyller krav og forventninger til samsvar mellom regulering og tilgangskriterier, kan det likevel være grunn til å forsøke å vurdere om noen prinsipper egner seg bedre enn andre. Dette kapitlet stiller opp en analytisk ramme for å vurdere autorisasjonsprinsippers egnethet. De ulike prinsippene kan være egnet for forskjellige hensyn i reguleringen, for eksempel slik at noen ivaretar pasienters medbestemmelse bedre, mens andre treffer bedre på taushetspliktbestemmelser, eller gjør det enklere å avdekke misbruk av tilganger. Forskjellig grad av egnethet kan også dreie seg om hva slags typer virksomheter et autorisasjonsprinsipp egner seg best for, eller om det fungerer bedre enn andre prinsipper ved samhandling på tvers av virksomhetsgrenser. I tillegg kan noen typer autorisasjonsprinsipper tenkes å fungere godt i samspill med hverandre, mens andre prinsipper nærmest har som forutsetning at de må være enerådende innenfor et informasjonssystem.

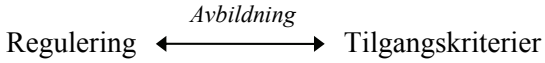
[734] De overordnede autorisasjonsprinsippene er presentert i kapittel 2.3.3 ovenfor.

Den analytiske rammen består av fem forskjellige vurderingskriterier. Disse vurderingskriteriene er konkretiseringer av elementer fra tidligere kapitler i avhandlingen, og ikke egentlig «nytt stoff», selv om terminologien etter hvert kanskje får et noe mer informatisk og teknokratisk preg. For å kunne fungere noenlunde instrumentelt som vurderingskriterier omfatter de ikke på langt nær så mange nyanser og forbehold som de bredere drøftingene tidligere i avhandlingen. Vurderingskriteriene er utvalg og forenklinger, konstruert for å kunne gjennomføre en overkommelig sammenligning av de ulike autorisasjonsprinsippene. De fem typene kriterier som er oppstilt kan stikkordsmessig betegnes som operasjonaliserbarhet, avbilding, medvirkning, etterprøvbarhet og teknologisk anvendelighet.



Operasjonaliserbarhet er et kriterium som dreier seg om det enkelte autorisasjonsprinsipps uttrykkskraft, og om hvilket handlingsrom det gir virksomhetene. Handlingsrom kan i denne sammenhengen være både positivt og negativt. Om ett bestemt prinsipp gir virksomhetene mange måter å operasjonalisere en bestemt del av reguleringen på, tyder det på at man har å gjøre med et prinsipp som kunne være egnet for flere ulike typer virksomheter. På den annen side vil forskjellige mulige operasjonaliseringer kunne innebære at det som i navnet er et ensartet prinsipp viser seg å være svært forskjellige ting i praksis.

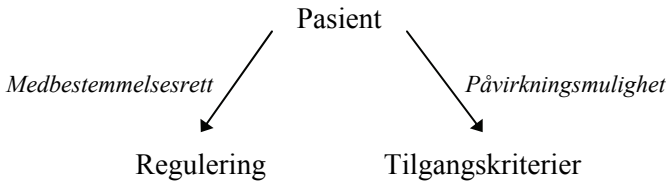
Det andre vurderingskriteriet er i hvilken grad et autorisasjonsprinsipp sørger for at tilgangskriteriene er en avbildning av reguleringen. I utgangspunktet er avbildning et vurderingskriterium som ikke innebærer noen fleksibilitet for virksomhetene. Ideelt sett vil et spørsmål om hvor godt et bestemt tilgangskriterium samsvarer med reguleringen ha samme svar uavhengig av trekk ved virksomheten, som for eksempel virksomhetens størrelse, oppgaver eller teknologiske utrustning.



I dette vurderingskriteriet går pilen begge veier. Avbildning kan ses som en generalisering av samsvarsbestemmelsen for tilgangskontroll i helseregisterloven, «… i samsvar med gjeldende

bestemmelser om taushetsplikt».[735] Kravet til samsvar vil være underoppfylt dersom tilgangskriteriene ikke gir noen brukbar representasjon av bestemmelser om taushetsplikt. I prinsippet kan avbildningen også overoppfylle samsvarskravet, dersom tilgangskriteriene er mer restriktive enn taushetspliktsbestemmelsene.

Det tredje vurderingskriteriet er to beslektede hensyn, som begge dreier seg om pasientens medinnflytelse over kontrollen med tilgang til og videreformidling av helseopplysninger. Enkelte former for medinnflytelse fra pasientens side er gjenstand for en rett til medbestemmelse. Et eksempel er sperring av journalen.[736] Pasienter kan også gis muligheter for å påvirke hvem som får tilgang, og under hvilke betingelser, utover det som er nedfelt som rettigheter.

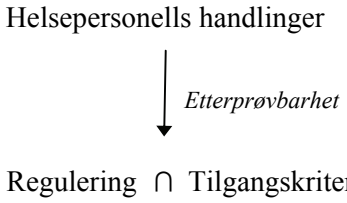


Begge former for pasientmedinnflytelse, altså uavhengig av om det er rettighetsfestet eller ikke, kan til en viss grad egne seg som grunnlag for tilgangskriterier som tvinges gjennom av en tilgangskontrollmekanisme. Det er imidlertid ikke slik at pasientmedinnflytelse nødvendigvis skal ivaretas gjennom tilgangskontroll. For eksempel er det ingenting i veien for at en pasients krav om å sperre en journal håndteres ved at journalen tas ut av det elektroniske journalsystemet, i stedet for at systemet håndterer sperringen. Den konkrete håndteringen av pasienters krav eller ønsker om å øve innflytelse over tilgang til opplysningene er således noe virksomhetene står relativt fritt til å bestemme selv. Pasientmedinnflytelse ligger derfor nærmere det som her er kalt operasjonalisering av virksomhetens egne beslutninger enn avbildning av regulering, selv om det i noen tilfeller dreier seg om klare rettigheter for pasienten.

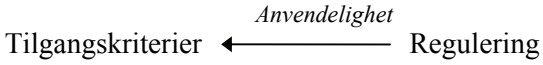
Det fjerde vurderingskriteriet er etterprøvbarhet. Både virksomhetens egen operasjonalisering av tilgangskriterier, og tilgangskriterienes direkte samsvar med reguleringen, munner ut i tilgangskriterier som overholdes eller brytes hver gang databrukeren leser, endrer eller videreformidler helseopplysninger. I den grad det ikke lykkes å tvinge gjennom et fullstendig samsvar mellom hva en databruker kan ha behov for å gjøre i IT-systemet, og samme

[735] Helseregisterloven § 13(1) annet punktum.
[736] Jf. kapittel 6.2.4.3 ovenfor.

databrukers praktisk mulige handlingsalternativer, er det en reell fare for brudd på regelverk eller tilgangskriterier.



Dersom man beveger seg utenfor skarpt definerte tilgangskriterier, som er i samsvar med den aktuelle reguleringen, kan det forekomme både legitime handlinger, i tråd med databrukernes plikter som helsepersonell, og mer lastefulle handlinger som bryter med det vernet pasienten skal ha. Etterprøvbarhet dreier seg ikke bare om å kunne avdekke at en handling, på utsiden av det opplagt godkjente, har funnet sted. Det dreier seg også om å kunne skille mellom hvilke av disse handlingene som likevel er legitime, og hvilke som ikke er det.



Teknologisk anvendelighet er et pragmatisk vurderingskriterium, og kan betraktes som en slags motvekt til de øvrige mer doktrinære vurderingskriteriene. Den teknologiske anvendeligheten er egentlig et vurderingskriterium som kan være svært omfattende i seg selv, for eksempel kan det omfatte både overensstemmelse med teknologiske standarder, robusthet og brukervennlighet. Som vurderingskriterium i denne sammenhengen er det ikke lagt opp til den typen håndfaste kvalitetsmål. Anvendelighet er her forenklet til en vurdering av om et autorisasjonsprinsipp er utbredt i praksis, og faglig anerkjent som et fornuftig svar på et spesifikt problem. Det er ikke nødvendigvis et klart samsvar mellom utbredelse og anerkjennelse. Gamle hevdvunne måter å gjøre ting på kan anses som utilstrekkelig, mens et autorisasjonsprinsipp som fremdeles er på eksperimentstadiet kan oppnå stor tilslutning i kunnskaps- og interessentmiljøer.

Som vurderingskriterium legges det ikke særskilt stor vekt på teknologisk anvendelighet, fordi hensikten med vurderingene av autorisasjonsprinsipper først og fremst er å sammenligne ideer og strategier, ikke å evaluere produkter. Det gir likevel en viss indikasjon om hvor tilgjengelige og praktikable de vurderte autorisasjonsprinsippene er.

8.1 Virksomheters operasjonalisering av reguleringen

Virksomhetene har en plikt til å etablere de tiltakene som trengs for å sikre tilstrekkelig vern mot urettmessig tilgang til eller videreformidling av helseopplysninger. Denne plikten kan i utgangspunktet ivaretas på en rekke ulike måter. Informasjonssikkerhetsreguleringen, og andre bestemmelser som har betydning for tilgang og videreformidling, gir primært anvisninger om hva som skal oppnås, mens føringene for hvordan dette skal eller kan oppnås er temmelig overordnede og generelle. Reguleringsmetoden krever imidlertid at virksomheten selv velger ut, detaljerer og konkretiserer tiltakene.[737]

Kravet til operasjonalisering innen et visst handlingsrom er mer flyktig, og vanskeligere å bruke instrumentelt, enn de øvrige vurderingskriteriene. For eksempel kan virksomhet A ha gode grunner for å ha mindre tillit til sine medarbeidere enn virksomhet B, og beslutte sine tilgangskriterier i tråd med det. På den annen side kan strammere tilgangskriterier i virksomhet A like gjerne være et uttrykk for at informasjonssikkerhetsarbeidet har større legitimitet der enn i virksomhet B. Det kan også tenkes at teknologivalgene i virksomhet A innebærer tilgangskontrollmekanismer som i stor grad determinerer valg av tilgangskriterier, mens virksomhet B har valgt teknologi som gir større frihet til å velge ulike typer tilgangskriterier. Operasjonaliserbarhet er dermed ikke et vurderingskriterium for å bedømme hva som gir «best mulig sikkerhet», men det sier noe om hvor godt en virksomhet vil kunne lykkes med å iverksette de tilgangskriteriene virksomheten selv har kommet frem til at er mest hensiktsmessige.

Det sentrale elementet i dette vurderingskriteriet er hvor godt et autorisasjonsprinsipp egner seg for at virksomheten skal kunne fastelegge tilgangskriterier som sikrer at tilgang «… bare gis i den grad dette er nødvendig for vedkommendes arbeid».[738] Dette er en ganske konvensjonell målsetning for et tilgangskriterium, og man trenger i utgangspunktet ikke å ha kjennskap til eller å ta hensyn til hvordan andre virksomheter har innrettet seg. I en liten og oversiktelig virksomhet kan det for eksempel legges opp til at tilganger tilordnes direkte til den enkeltperson som har behovet. I større virksomheter, der organiseringen av arbeidet er mindre personavhengig, er det mer hensiktsmessig for eksempel å knytte tilganger til trekk ved den ansattes funksjoner, pasientbehandlingen eller informasjonsstrukturen.

Et annet og mer komplekst element ved dette vurderingskriteriet er egnethet for å sikre god nok sammenheng i tilgangskriteriene på tvers av virksomhetsgrenser, i de situasjonene der det

[737] Jf. kapittel 4, risikobasert internkontroll som reguleringsmetode.
[738] Helseregisterloven § 13(1) annet punktum (første del av setningen).

kan gis anledning til det.[739] Det kan etableres ulike styringsmodeller, som innebærer noe ulike måter å operasjonalisere tilgangskriterier på, for å ivareta informasjonssikkerhet på tvers av virksomhetsgrenser. Den modellen som ligger nærmest tradisjonelle metoder og standarder for informasjonssikkerhet er å gjøre avgiverens virksomhetsinterne operasjonalisering av tilgangskriterier direkte gjeldende for de samarbeidende virksomheter som får tilgang til opplysningene. Ved å eksportere avgivende virksomhets tilgangskriterier til virksomheter som samarbeider, forblir dette en del av virksomhetens lokale sikkerhetsarbeid. Dermed blir sikkerhetsarbeidet i mindre grad rammet av et av de generelle problemene som er påpekt om internkontroll som reguleringsmetode, at den er lite egnet for å ivareta et samfunnshensyn på tvers av virksomhetsgrenser.[740]

En myk måte å gjøre avgivers tilgangskriterier gjeldende på, er å inngå avtaler mellom virksomhetene om hvordan dette skal foregå. Det er en myk metode i den forstand at den ikke iverksettes med effektive teknologiske mekanismer som tvinger gjennom tilgangskriteriene. Skulle man derimot ønske teknologiske mekanismer for å tvinge gjennom avgivers tilgangskriterier, må informasjonselementer kunne merkes med representasjoner av disse kriteriene. En generell betegnelse som kan brukes om slike mekanismer er «klebrig tilgangspolitikk», som er en slags oversettelse av uttrykket *sticky policies*.[741] Hensikten er at opplysningene frakter med seg tilgangskriteriene, og fortsetter å tvinge dem gjennom etter at opplysningene er videreformidlet til en annen virksomhet og eventuelt til et annet IT-system. Prinsipielt sett har klebrighet en del til felles med sikkerhetsgraderinger, der den merkingen som påføres er bindende for alle som er involvert i behandling av informasjonen.[742] Ved behandling av helseopplysninger er det imidlertid behov for mer varierte og dynamiske måter å angi tilgangskriterier på enn statiske graderinger.

Det er to sentrale spørsmål som melder seg dersom avgivers tilgangskriterier skal gjøres bindende for samarbeidende virksomheter. Det ene spørsmålet er hvilke typer opplysninger et tilgangskriterium skal knyttes til. Det kan reguleres relativt åpent, for eksempel ved at en

---

[739] For *behandlingsrettede* helseregistre oppstiller helseregisterloven noen få, forskjellige metoder og kriterier for tilgang til og bruk av helseopplysninger over virksomhetsgrenser, jf. kapittel 5.2.2.
[740] Jf. kapittel 4.5.3 ovenfor.
[741] Begrepet «sticky policies» har tidligere vært brukt innen statsvitenskap, som et overveiende negativt uttrykk, om treghet eller motkrefter til teknokratisk reformiver, jf. Bent Sofus Tranøy (2000): «Losing credit. The politics of liberalisation and macro-economic regime change in Norway 1980-92 (99)», s. 71. I informatisk teori, om dataorientert tilgangskontroll og personvernøkende teknologier i heterogene systemmiljøer, er klebrighet en positiv egenskap. Jf. betegnelsen «sticky policies paradigm», blant annet i Günter Karjoth m. fl. (2003): «Platform for Enterprise Privacy Practices: Privacy-Enabled Management of Customer Data». I: *Privacy enhancing technologies : second international workshop, PET 2002, San Francisco, CA, USA, April 14-15, 2002 : revised papers*, s. 194–198.
[742] Jf. sikkerhetsloven § 11.

henvisning eller en bestemt type diagnose skal innebære at bare bestemte yrkesgrupper eller avdelinger i samarbeidende virksomheter får tilgang til opplysninger om den aktuelle pasienten. En mer restriktiv mulighet er å avgrense også hvilke deler av pasientens journal man får tilgang til, ut fra formålet med samhandlingen.[743] Dersom en klebrig tilgangspolitikk skal kunne ivareta pasientens handlingsvalg, må også informasjon om eventuelle samtykker og sperringer være tilgjengelig for samarbeidende virksomheter i den utstrekning det kan ha betydning for berettigelsen av tilgang.

Det andre spørsmålet som melder seg er hvordan man kan sikre seg at samarbeidende virksomheter føler seg bundet av, og faktisk respekter, de klebrige kriteriene. Antakelig er det vanskelig å komme utenom en eller annen form for revisjon som gjennomgår tilganger i flere samarbeidende virksomheter i sammenheng. Det er kanskje også mulig å se for seg noe i retning av testprosedyrer og testsystemer, for å forhåndsverifisere at informasjonssystemet i virksomhet B lykkes i å håndheve klebrige kriterier fra informasjonssystemet i virksomhet A. Valg av strategi for å sikre at tilgangskriteriene faktisk respekteres i et samarbeid blir imidlertid ikke tillagt vekt i dette vurderingskriteriet.

En annen tilnærming til å sikre god nok sammenheng i tilgangskriteriene på tvers av virksomhetsgrenser er å etablere felleskriterier. Felles tilgangskriterier fastlegges ikke gjennom avgiverens sikkerhetsarbeid, men besluttes og forvaltes av et konsortium som deltakende virksomheter gir fullmakt til, eller av en sentral aktør utenfor virksomhetene.[744] I utgangspunktet innebærer det en svekkelse av virksomhetenes handlingsrom. Dette er mest aktuelt der mange og forskjelligartede virksomheter har behov for å dele helseopplysninger. Felles tilgangskriterier forutsetter enten en sterk standardisering av informasjonsstrukturer og opplysningstyper, for at tilgangskriteriene skal bety det samme i ulike typer virksomheter, eller at man avstår fra nyanserte og dynamiske tilgangskriterier, altså slik at de blir mindre presise. Enda mer problematisk enn standardisering av informasjonen, er spørsmålet om hvorvidt felles tilgangskriterier må baseres på forutsetninger om hvordan en virksomhet er organisert. For eksempel kan et kriterium som sikrer tilgang for en bestemt rolle innebære at det som er en rimelig avgrensning av hvilke databrukere som får tilgang i virksomhet A, fører til at alle eller ingen får tilgang i virksomhet B, dersom det aktuelle rollebegrepet ikke representerer noe meningsfullt i begge virksomheter. Rene felleskriterier, for å dele opplysninger mellom mange virksomheter av ulike slag, kan dermed vanskelig bli særlig nyanserte.

[743] Jf. kapittel 5.1.1.2 ovenfor, om strukturering av journal.
[744] Se nærmere om disse styringsmodellene i kapittel 5.2.2.5 ovenfor.

Det kan også være aktuelt med ulike former for hybrider mellom klebrige kriterier og felleskriterier.[745]

8.2 Tilgangskriterier som avbilder helserettslig regulering

De sidene ved den helserettslige reguleringen som først og fremst påvirker tilgangskriterier er bestemmelser om taushetsplikt, herunder også bestemmelser om unntak fra taushetsplikt. Noen av unntakene fra taushetsplikt beror på, eller åpner for, pasienters medbestemmelse. Grunnlaget for at disse bestemmelsene er et relevant vurderingskriterium, er samsvarsbestemmelsen i helseregisterloven.[746]

Begrepet avbildning er her et litt mattere uttrykk enn «speiling», som er brukt i forarbeid til pasientrettighetsloven, om et lignende krav til samsvar med gjeldende bestemmelser om taushetsplikt: «Opplysninger om legems- og sykdomsforhold samt andre personlige opplysninger skal behandles i samsvar med gjeldende bestemmelser om taushetsplikt.»[747] I kommentar til denne bestemmelsen i proposisjonen til pasientrettighetsloven het det:

> Første ledd speiler de generelle taushetspliktsbestemmelsene etter ny lov om helsepersonell § 21. Personvernhensyn tilsier imidlertid at adgangen til å utlevere følsomme helseopplysninger til andre enn den opplysningene gjelder, bør være snever. Vern mot spredning av opplysninger går til enhver tid like langt som helsepersonellets taushetsplikt.[748]

Mens det å speile, i dette sitatet, er uttrykk for likt omfang og meningsinnhold, er ordet avbildning valgt her som en forsiktig innsigelse mot å tillegge samsvarsbestemmelsen i helseregisterloven en tilsvarende direkte speilingsfunksjon. Det er særlig to grunner som taler mot å forstå også helseregisterlovens samsvarbestemmelse som direkte speiling. For det første er aktørkonstellasjonene forskjellige. Helsepersonelloven og pasientrettighetsloven er grunnleggende sett på samme nivå, og uttrykker relativt oversiktlige deontiske relasjoner.[749] Selv om virksomhetene er til stede i form av et «sørge for»-ansvar, speiles helsepersonells taushetsplikt direkte mot pasientens vern mot spredning av opplysninger. I helseregisterlovens

[745] Et mer overordnet teoretisk fundament for tilgangskriterier som kan kombinere de ytre rammene fra en sentral aktør med de enkelte virksomheters operasjonaliseringer innen et visst handlingsrom er drøftet i kapittel 2.2.3 ovenfor, særlig med henvisning til artikkelen Jones og Sergot (1996).
[746] Helseregisterloven § 13(1) annet punktum.
[747] Pasientrettighetsloven § 3-6 første punktum. Overskriften til denne bestemmelsen i pasientrettighetsloven er *«Rett til vern mot spredning av opplysninger.»*
[748] Ot.prp. nr. 12 (1998-1999), s. 131.
[749] Plikt/rettighet eller frihet/ikke-rettighet, jf. hohfeldske rettighetsrelasjoner, kapittel 2.2.1 ovenfor.

samsvarsbestemmelse er det en konjunksjon som involverer både databrukeren, som er den som har taushetsplikt, og virksomheten, som gir tilgang og beslutter hva som er nødvendig for vedkommendes arbeid. I utgangspunktet er dette en over- og underordningsrelasjon.[750] Databrukerens underordning er likevel noe tvetydig, han blir ikke på noe vis fritatt fra taushetsplikten overfor pasienten selv om virksomheten skulle tildele unødvendig vide tilganger.

Den andre grunnen som taler mot å forstå helseregisterlovens samsvarsbestemmelse som krav til direkte speiling, er spørsmålet om hva det er praktisk mulig å oppnå. Dersom tilgangskriteriene skal «si det samme» som taushetspliktbestemmelsene, kan det kreve så mye av organisatoriske skranker, tidsbruk og håndtering av tilleggsopplysinger som innhentes kun for å styre håndteringen av helseopplysninger, at det verken tjener helsehjelpen eller personopplysningsvernet. Det er derfor både slutningsmessig og praktisk rimelig å tolke helseregisterlovens samsvarsbestemmelse slik at tilganger skal gis ut fra en hensiktsmessig kombinasjon av virksomhetens operasjonaliseringer og gjeldende bestemmelser om taushetsplikt. Det innebærer igjen et mer relativisert krav til samsvar, slik at uttrykket avbildning er mer treffende enn speiling. Vurderingskriteriet avbildning dreier seg om hvor godt, og under hvilke forutsetninger, et autorisasjonsprinsipp egner seg for å uttrykke samsvar mellom gjeldende bestemmelser om taushetsplikt og tilgangskriterier.

En hovedregel om taushetsplikt, i et behandlingsrettet helseregister, innebærer at helseopplysninger skal være tilgjengelige for den som har dokumentert dem. Utover dette dreier avbildningen seg om å formalisere unntaksbestemmelsene. De relativt mange unntakene fra helsepersonells taushetsplikt er formulert på ulike vis, men de inneholder også noen fellestrekk i hvordan unntaksbestemmelsene er bygd opp.[751] Som vurderingskriterium, for hvorvidt et tilgangskriterium kan sies å være en noenlunde grei avbildning av bestemmelsen, er det noen få kategorier av slike fellestrekk som er særlig relevante. Den første kategorien er unntaksbestemmelsens modalitet. Hovedinndelingen er opplysningsrett, som er kan-bestemmelser, og opplysnings- og meldeplikter som er skal-bestemmelser. Det finnes imidlertid flere nyanser av disse modalitetene. Nyansene har sammenheng med andre trekk ved unntaksbestemmelsene, som initiering, vilkår, og pasientens eventuelle rett til medbestemmelse over unntakssituasjonen.

[750] Til forskjell fra pasientrettighetslovens samsvarsbestemmelse ligner samsvarbestemmelsen etter helseregisterloven mer på den hohfeldske relasjonen kompetanse/avhengighet, jf. kapittel 2.2.1 ovenfor.
[751] Unntaksbestemmelsene er nærmere beskrevet og plassert i en systematisk sammenheng i kapittel 6.3.1.2 ovenfor.

Det vil være relativt enkelt å stille opp tilgangskriterier for en skal-bestemmelse, dersom det verken er vilkår som skal vurderes, krav til at pasienten samtykker, eller mulighet for å komme med innsigelser. Mange av bestemmelsene angir imidlertid vilkår i en eller annen form. De fleste bestemmelser om unntak fra taushetsplikt forutsetter at noen må vurdere hvorvidt den situasjonen som gjør unntak fra taushetsplikten nødvendig, faktisk har inntrådt. Til sammenligning er det i utgangspunktet relativt få unntaksbestemmelser som gir pasienten medinnflytelse. Samtykke er en forutsetning på enkelte omfattende områder som opplysninger til forsikringsselskap, og de fleste situasjoner der det skal gis opplysninger til sosialtjenesten. I tillegg er krav til samtykke hovedregelen ved bruk av helseopplysninger i medisinsk og helsefaglig forskning. Selv om det i utgangspunktet skulle være enkelt å konstatere om et samtykke er gitt eller ikke, blir bildet mer komplisert når man har behov for en etterrettelig angivelse av samtykkets rekkevidde, og for en klar forståelse av hvordan man skal håndtere situasjoner der et samtykke trekkes tilbake.

Når opplysninger skal gis til samarbeidende helsepersonell, fordi det er nødvendig for å yte helsehjelp, er det et presumert samtykke, eller en innsigelsesrett, som gjelder. Selv om uttrykkelige og presumerte samtykker ligner hverandre på den måten at begge gir pasienten en mulighet til å bestemme selv, blir dette to temmelig ulike mekanismer når de skal transformeres til tilgangskriterier. Ved et uttrykkelig samtykke er det tillatelsen, altså aksept for at unntak fra taushetsplikten skal gjelde, som representeres. Ved et presumert samtykke representeres innsigelsen, som en stoppordre for den unntaksbestemmelsen som er påberopt.

Initiering dreier seg om hvem som setter i gang den bevegelsen av helseopplysninger som gjør det påkrevd å ta stilling til om taushetsplikt, og deretter et mulig unntak, kommer til anvendelse. De som skal eller kan initiere er oftest noenlunde klart angitt i lov, for eksempel helsepersonellet selv, samarbeidende helsepersonell, barneverntjeneste, forsikringsselskap, tilsynsorgan, departement med flere. I en del sammenhenger er det mer indirekte angitt, for eksempel ved forskriftsbestemmelse om hvem som er databehandlingsansvarlig for et bestemt register som det gjelder en meldeplikt til. Generelt er det lite problematisk å definere tilgangskriterier for avgiverinitierte unntak fra taushetsplikten, altså der vedkommende helsepersonell skal vurdere noe av eget tiltak. En slik vurdering har i praksis allerede funnet sted når avgiveren bestemmer seg for å gi noen tilgang til opplysningene. Tilgangskriterier for slike situasjoner skal primært sikre transparens og etterprøvbarhet.

Når det er den som har behov for opplysningene som initierer, er to forskjellige strategier for å håndtere vurderingene mulige. Den ene, som ligger nærmest dagens praksis, er forespørsler, der behovet begrunnes, hvorpå spørsmålet om tilgang vurderes og besvares av den

som har taushetsplikten. Det innebærer for det første en forsinkelse, som hindrer direkte tilgang. For det andre kan det være arbeidskrevende dersom volumet blir stort, slik at arbeidsomfanget i seg selv kan bli et hinder for informasjonsdeling som både er berettiget og hensiktsmessig. Den andre strategien er forhåndsvurderinger av informasjonen, for å ta stilling til om den egner seg for deling, eventuelt med hvem, til hvilke formål, og på hvilke vilkår.[752] Realiteten i å legge opp til forhåndsvurderinger vil være en dreining av taushetspliktens innretning, til at den i større grad blir et anliggende for virksomheten, og i tilsvarende mindre grad et personlig anliggende for det helsepersonellet som har dokumentert opplysningene. Selv om man skulle velge å legge opp til at den som dokumenterer også utfører forhåndsvurderingen, blir det likevel i praksis noe som virksomheten må tilrettelegge for, og ha en viss kontroll med. Å forhåndsvurdere hvilke opplysninger som skal kunne falle inn under et unntak fra taushetsplikten vil ligne mer på virksomhetens operasjonalisering av tilgangskriterier enn på avbildning av taushetspliktbestemmelser. Dermed er det enklere å uttrykke holdbare kriterier for mottakerinitiert tilgang dersom man velger å basere disse kriteriene på forhåndsvurderinger. Man kan også si det slik at forhåndsvurderinger vil gjøre kravet til samsvar med gjeldende bestemmelser om taushetsplikt noe mer hult.

Som vurderingskriterium vil avbildning dreie seg om en samlet vurdering av hvor godt et autorisasjonsprinsipp egner seg for å uttrykke bestemmelser om taushetsplikt med tilhørende unntaksbestemmelser.

8.3 Sammenligning mellom operasjonalisering og avbildning

Blant de fem vurderingskriteriene står de to første, operasjonaliserbarhet og egnethet for å avbilde regulering, i en særstilling. De tre øvrige vurderingskriteriene som presenteres i dette kapitlet kan kanskje vise seg like tungtveiende i praksis. De to første rommer imidlertid også en mer fundamental teoretisk forskjell, som denne avhandlingen har nærmet seg fra litt ulike vinkler.

En innfallsvinkel til forskjeller mellom operasjonalisering og avbildning er av teknologisk art. Det første vurderingskriteriet peker i retning av statiske tilgangskriterier, det andre peker mer i retning av dynamiske kriterier.[753] Tilgangskriterier som virksomheten selv beslutter, innenfor et relativt stort handlingsrom, kan representere trekk ved organiseringen, oppgavene

[752] Forhåndsvurderinger er et av temaene som drøftes i Ot.prp. nr. 51 (2008-2009), s. 35. Dette temaet er også berørt i to litt forskjellige sammenhenger tidligere i avhandlingen, henholdsvis kapittel 5.1.1.2 og 6.2.2.2.
[753] Jf. kapittel 2.3.2 ovenfor.

og opplysningene. Tilganger gis eller avslås uavhengig av detaljert kunnskap om den konkrete situasjonen som berettiger tilgang til opplysningene. Både modeller for tilgangskriterier som bygger på gradering av informasjon og sikkerhetsklarering av databrukere, og modeller som bygger på hvilke typer opplysninger som gjøres tilgjengelige for en ansatt med bestemte oppgaver, eller med en bestemt organisatorisk tilhørighet, er forholdsvis statiske. Selv om tilgangskriteriene kan endres, i medhold av besluttede rutiner for å gjennomføre slike endringer, er det prinsipielt sett mulig å svare på om databruker D har tilgang til opplysning O om pasient P, uavhengig av om det konkrete behovet allerede har oppstått eller ikke. Et statisk tilgangskriterium «eksisterer» som en entitet, ved at det er truffet en tilgangsbeslutning som kan identifiseres og endres.

Tilgangskriterier som skal avbilde gjeldende bestemmelser om taushetsplikt vil ofte være avhengige av opplysninger som ikke er tilgjengelige fra før, og som kanskje heller ikke ville ha blitt generert dersom det ikke var fordi man skulle undersøke berettigelsen av tilgang. Selv om tilgangskriteriene skulle ligge fast, er det ofte umulig å svare på om databruker D' har tilgang til opplysning O' om pasient P' før det konkrete behovet har oppstått. Tidspunktet for når det er mulig å evaluere om tilgang skal gis eller ikke kan komme svært nær opptil det tidspunkt hvor databrukeren faktisk har behov for opplysningene. Vurderingen av om det er nødvendig at helseopplysninger gis til samarbeidende helsepersonell fastslås i noen tilfeller flere uker i forveien, mens det i andre tilfeller er et behov som oppstår plutselig. Både den vage avgrensningen av hvilken kunnskap om en situasjon som kan inngå i konkrete tilgangsvurderinger, og at tilgangsvurderingen ikke alltid er mulig å gjennomføre særlig lang tid i forveien, peker i retning av at avbildning gir mer dynamiske tilgangskriterier. Et dynamisk tilgangskriterium har ikke nødvendigvis samme form for selvstendig eksistens som et statisk tilgangskriterium. Det er naturligvis truffet en beslutning om et autorisasjonsprinsipp, men de enkelte tilganger er ikke nødvendigvis identifiserbare annet enn som representerte slutningsregler. Selve tilgangen til bestemte opplysninger har ikke i konkret forstand blitt «tildelt».

En annen innfallsvinkel til forskjeller mellom operasjonalisering og avbildning er at de er basert på ulike reguleringsmetoder.[754] Operasjonalisering uttrykker virksomhetens egne beslutninger, med både rett og plikt for virksomheten til å vurdere selv hvilken risiko som er påregnelig og hvordan den skal håndteres. En avbildning av gjeldende bestemmelser om taushetsplikt skal derimot i prinsippet være universell. Litt firkantet sagt har det tilgangskriteriet

[754] De konkrete forskjellene kommer særlig til uttrykk i drøftingene av personopplysningsrettslig regulering av informasjonssikkerhet i kapittel 6.2.4.1, med nærmere redegjørelse for den teoretiske bakgrunnen i kapittel 4, og helserettslig regulering av taushetsplikt i kapittel 6.3.1 ovenfor.

som gir samme resultat som en domstol ville ha kommet til i en konkret situasjon, løst det konkrete spørsmålet bedre enn et tilgangskriterium som gir et annet resultat.[755]

Disse to innfallsvinklene synliggjør et lite tankekors: Den mest fleksible reguleringen legger grunnlaget for de mest statiske tilgangskriteriene, fordi reguleringen skal operasjonaliseres, dokumenteres og kunne forsvares uavhengig av om et konkret behov for tilgang har oppstått. Den reguleringen som gir virksomhetene minst handlingsrom kaller på mer dynamiske tilgangskriterier, fordi avbildningen av taushetspliktbestemmelser tilsier at det enkelte behov for tilgang vurderes ut fra en mer detaljert kunnskap om den situasjonen som berettiger tilgangen. Dette lille paradokset utgjør imidlertid ikke noen ny og selvstendig problematisering av forskjellene mellom operasjonalisering og avbildning, det understreker en forskjell som er gjennomgående i hele avhandlingen.

8.4 Medbestemmelsesrett og påvirkningsmuligheter

En av de mest omfattende mulighetene en pasient har til å påvirke tilgang til opplysninger om seg selv, er at helsepersonell kan få opplysningsrett i den grad pasienten samtykker til det.[756] Det er en form for medinnflytelse som er nært knyttet til taushetspliktbestemmelsene, og derfor heller hører hjemme under vurderingskriteriet avbildning ovenfor. De formene for medbestemmelsesrett og påvirkningsmuligheter som inngår i vurderingskriteriet medinnflytelse her, er ikke nødvendigvis forbundet med helseregisterlovens kriterier for hva som skal til for at en person skal kunne gis tilgang til helseopplysninger.[757] Dette vurderingskriteriet dreier seg om hvorvidt et autorisasjonsprinsipp har egenskaper som i seg selv er egnet for å ivareta pasientens autonomi eller personopplysningsvern, uavhengig av om det i direkte forstand kan gjøres gjeldende som oppfyllelse av det reguleringen krever. Å tilføre autorisasjonsprinsipper slike egenskaper, kan betraktes som et bidrag til personvernøkende, eller

[755] Dette er et eldre og mer innarbeidet perspektiv enn den fleksible reguleringen som belegges i kapittel 4. Prediksjon, som uttrykk for hva som er rett, er godt beskrevet i Oliver Wendell Holmes (1897): «The Path of the Law». I: *Harvard Law Review,* s. 457–478: «The object of our study, then, is prediction, the prediction of the incidence of the public force through the instrumentality of the courts» (s. 457). Det oppsummeres litt mindre formelt, men like elegant: «The prophecies of what the courts will do in fact, and nothing more pretentious, are what I mean by the law» (s. 461).
[756] Helsepersonelloven § 22.
[757] Helseregisterloven § 13(1) annet punktum.

personvernvennlige, teknologier.[758] Tilgangskriteriene som det da vil dreie seg om hører hjemme under betegnelser som e-helse og «den aktive pasient».

Enkelte spesifikke rettigheter for pasienter kan ha stor betydning for behandlingen av helseopplysninger, uten at de passer særlig godt inn i de øvrige vurderingskriteriene. Noen eksempler, som er omtalt tidligere, er retten til å sperre journalen, retten til ikke å vite, rett til individuell plan og rett til fornyet vurdering.[759] Andre aktuelle påvirkningsmuligheter, som ikke er like klart forankret i bestemte rettigheter, er en mulighet for å bestemme hvilke enkeltpersoner blant de ansatte ved et sykehus som ikke skal få tilgang til journalen.[760] Videre kan pasienter ha et ønske om at helsepersonell skal få se enkelte deler av de opplysningene annet helsepersonell har dokumentert, også når dette ikke er direkte berettiget ut fra den helsehjelpen som ytes. Et annet mulig ønske fra pasienten er å få supplere de opplysningene som er nedtegnet som dokumentasjon av helsehjelpen, med egne opplysninger.

Medinnflytelse er et vurderingskriterium som handler om hvorvidt et autorisasjonsprinsipp gir støtte for tilgangskriterier som slipper til pasienten. I utgangspunktet er det plausibelt at det å åpne for pasientens medvirkning er gunstig, og at det gir en positiv opplevelse av styrket autonomi. Likevel er det nødvendig å ta med i betraktningen et behov for å sikre et tilstrekkelig personopplysningsvern også for pasienter som lar være å utøve aktiv medinnflytelse. Muligheter for medinnflytelse bør med andre ord først og fremst fungere som supplement til andre tilgangskriterier.

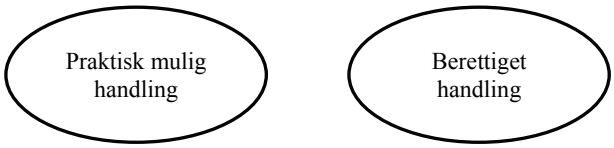
8.5 En overtredelsestaksonomi for etterprøvbarhet

For å vurdere om et autorisasjonsprinsipp er egnet for å uttrykke tilgangskriterier i tråd med den relevante reguleringen, kan det også være hensiktsmessig å undersøke hvordan man kan fange opp handlinger som eventuelt er i strid med de representerte tilgangskriteriene.[761] Et autorisasjonsprinsipp som gir gode muligheter for å avdekke og reagere på unødvendige eller uberettigede tilganger, vil i utgangspunktet innebære bedre kontroll med tilgangene enn de prinsippene hvor det er vanskeligere å etterprøve det som gjøres. Etterprøvbarhetens fortrinn

[758] Personvernkommisjonen manet i sin rapport til å utrede mer *personvernvennlig* bruk av elektronisk pasientjournal, før man begynner å gi tilgang på tvers av foretak. NOU 2009:1, s. 182–183.
[759] Jf. kapitlene 6.2.4.3 og 6.3.2.1 ovenfor.
[760] Slike funksjoner finnes i praksis på visse områder. En muntlig kilde omtalte dette som «svigermorfilter».
[761] En annen tilnærming til dette, som er bredere anlagt enn denne avhandlingens perspektiv som er kontroll med handlingene til databrukere som i utgangspunktet skal ha tilgang til opplysninger, finnes i Lillian Røstad (2006): «An extended misuse case notation: Including vulnerabilities and the insider threat» (konferanseartikkel).

må selvfølgelig ha en slags logisk grense: Tilgangskontrollen kan neppe sies å være i tråd med reguleringen dersom ingen gale handlinger avverges på forhånd, selv om man skulle lykkes i å rydde opp i alt etterpå.[762]

Et utgangspunkt for å vurdere etterprøvbarhet, er å se nærmere på hva slags ulike typer brudd på tilgangskriteriene som er mulige eller sannsynlige. En inndeling i og beskrivelse av slike typer kan kalles en overtredelsestaksonomi.[763] En innledende illustrasjon, for å motivere taksonomien, er å skille mellom handlinger som det er praktisk mulig for databrukere å gjennomføre, og handlinger som er berettigede ut fra et eller annet grunnlag.



Figur 7 Mulig versus berettiget handling

De praktisk mulige handlingene er de handlinger som kan utføres i et IT-system, og som ikke blir forhindret av implementerte, tekniske tilgangskontrollmekanismer. En berettiget handling omfatter både det man har plikt til å gjøre og det man har frihet til å gjøre.[764] Dersom man skulle tenke seg en idealsituasjon, et nøyaktig samsvar mellom regulering og kontroll, ville ovalene i illustrasjonen ovenfor overlappet hverandre fullstendig. Det ville se ut som ett symbol, teksten kunne være praktisk=berettiget. Alle de autorisasjonsprinsippene som vurderes i denne avhandlingen har en større eller mindre, men ikke fullstendig, overlapping.

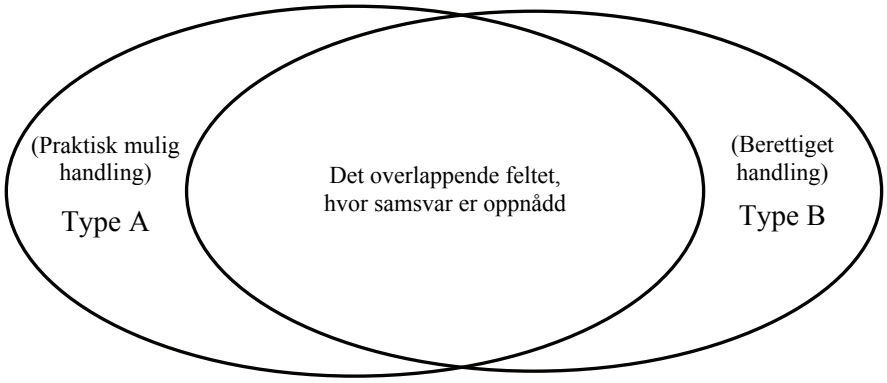
Handlinger som havner utenfor det sammenfallende området kan havne både i feltet for praktisk mulige handlinger, og i feltet for berettigede handlinger. For så vidt kan en handling også havne utenfor begge disse feltene, slik tilfellet for eksempel vil være ved et eksternt

[762] Enkelte forskere har argumentert godt for at kompleksiteten i tilgangskriterier er så høy at en rendyrket etterhåndskontroll er den beste måten å håndtere tilganger på. Se for eksempel Dean Povey (1999): «Optimistic security: a new access control paradigm» (konferanseartikkel) eller Daniel J. Weitzner m. fl. (2008): «Information accountability». I: *Communications of the ACM,* s. 82–87. Det er imidlertid neppe en holdbar måte å uttrykke tilgangskriterier i tråd med den reguleringen som gjelder for helseopplysninger i Norge.

[763] En taksonomi er i denne sammenhengen en strukturering og navnsetting av noen typer handlinger. Uttrykket taksonomi brukes på samme måte som, og inspirert av, artikkelen Carl E. Landwehr m. fl. (1994): «A taxonomy of Computer Program Security Flaws». I: *ACM computing surveys,* s. 211–254.

[764] Dette skillet kan ses som en parallell til det noe mer generelt anlagte begrepsparet *ability space* og *liberty space*, i Lindahl (2005). Samme forfatter har også tidligere formalisert en slik inndeling, som to varianter av den deontiske modaliteten *kan,* med betegnelsen CAN-P for det man har praktisk mulighet til å gjøre, og CAN-J for det man kan være berettiget til å gjøre. Lars Lindahl (1977): *Position and change: a study in law and logic*, s. 194–197.

angrep.[765] En justert utgave av skissen viser hvordan en ufullstendig overlapping kan gi to ulike hovedtyper av overtredelser.



Figur 8 Overtredelser type A og type B

Det er vesentlige forskjeller mellom hovedkategoriene, type A og type B, i taksonomien. Overtredelser av type A innebærer at databrukeren har handlet i strid med regler og retningslinjer, men uten å bryte en teknisk barriere mot tilgang. Vedkommende er altså i teknisk forstand autorisert, men uten at tilgangen er berettiget. Dersom en handling hører til under type A, er det helt klart at det som har foregått ikke skulle ha vært gjort. Overtredelser i felt B innebærer at man utfører en handling som er berettiget, men må trosse en teknisk barriere for å gjennomføre det. Databrukeren er altså ikke autorisert, i den betydningen dette begrepet har innen tilgangskontrolldisiplinen. En handling under type B vil svært ofte være noe som helsepersonell skal eller bør gjøre, selv om det også vil kunne forekomme visse situasjoner der man bør la være å utføre en handling som man formelt sett har frihet til å utføre. Grunnen til at type B likevel hører hjemme i en slik taksonomi, er at databrukeren må ty til en eller annen form for omgåelse, fortrinnsvis i en form som virksomheten aksepterer, for å få utført den berettigede handlingen. Hver av disse kategoriene kan kanskje beskrives litt uhøytidelig med hver sin «gjerningsmannsprofil», med en klisjé fra kriminalsjangeren, der databrukerne i felt A er «bad guys» mens de i felt B er «good guys who need to cut corners».

Som et generelt utgangspunkt kan man si at det primært er pasientens personopplysningsvern som står på spill i type A, mens det også kan være pasientens helse som står på spill i type B. I praksis er dette imidlertid noe mer nyansert. En eventuell tvil om hvor holdbar berettigelsen egentlig er, vil dreie seg om pasientens personopplysningsvern. En omgåelse av sikkerhetsfunksjonalitet, selv når det er nødvendig for å yte helsehjelp, må være etterprøvbar

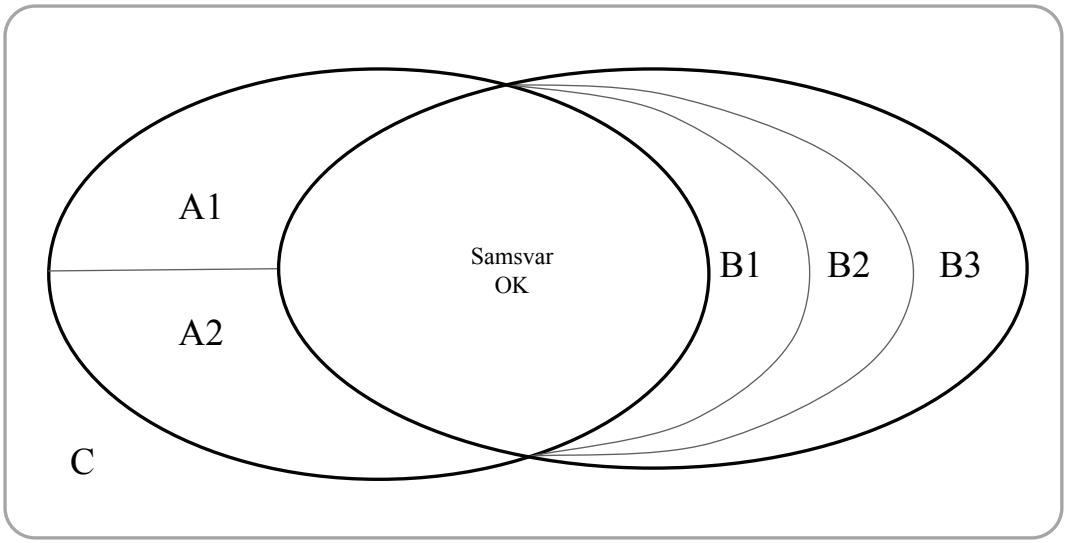
[765] Eksterne angrep ligger i utgangspunktet utenfor avhandlingens problemstilling. Likevel kan en slik «utenforposisjon» ha en viss relevans for å drøfte gråsoner i taksonomien.

dersom man skal kunne opprettholde den generelle tilliten til virksomhetens informasjonssikkerhetsarbeid.

De to hovedtypene av overtredelser kan deles inn i litt mer spesifiserte underkategorier. Type A kan deles inn i to varianter av å misbruke en teknisk tilgangsmulighet. Den ene, A1, er uberettiget tilegnelse av helseopplysninger uten at disse nødvendigvis bringes videre.[766] Den andre typen, A2, er videreformidling av opplysninger i strid med taushetsplikten, altså et taushetspliktbrudd i mer konvensjonell forstand.

Til forskjell fra de relativt skarpt avgrensede variantene under type A, kan overtredelser av type B kanskje heller betraktes som inndelt i underkategorier ut fra hva slags metode man bruker for å omgå de generelle barrierene. Overtredelser av type B kan tentativt deles inn i tre underkategorier, som har ulik grad av avstand fra det som virksomheten kan føre kontroll med og innlemme i ordinær avvikshåndtering i sikkerhetsarbeidet. Den første underkategorien, B1, som ligger nærmest virksomhetens ordinære arbeid med å operasjonalisere og uttrykke tilgangskriterier, kan betegnes som virksomhetsinitierte aktualiseringsmekanismer. Behovet for tilgang fastlegges dynamisk, og tilgangen som sådan er en ad hoc utvidelse av de generelle kriteriene, men følger fastlagte rutiner under virksomhetens kontroll. Den andre kategorien, B2, er selvautorisering, gjerne betegnet som en form for nødrettstilgang. I slike tilfeller kan helsepersonellets egen vurdering være en overprøving av virksomhetens kriterier. Denne formen for omgåelse er imidlertid også innenfor et tilrettelagt rammeverk, handlingen er registrert, og berettigelsen av tilgangen kan tas opp til vurdering i ettertid. Den tredje kategorien, B3, er klare og bevisste brudd på teknisk autorisasjon, ved bruk av metoder som bryter med grunnleggende sikkerhetsprinsipper. Det kan for eksempel være tyveri eller lån av andres passord, eller direkte lesing eller manipulering av datafiler uten å bruke tilrettelagte brukergrensesnitt, med videre.

[766] Såkalt «snoking», jf. kapittel 6.3.1.3 ovenfor.



Figur 9 Detaljert inndeling av type A og type B

Illustrasjonen ovenfor viser den prinsipielle forskjellen i inndelingen av underkategorier til type A og type B. Mens A1 og A2 er to ulikt motiverte misbruk av en tildelt autorisasjon, følger B1, B2 og B3 en skala fra mer til mindre etterprøvbare måter å omgå en manglende autorisasjon på.

En mulig gråsone mellom type A og type C, som altså er sikkerhetsovertramp utenfor begge disse sfærene, kan oppstå der et IT-system har svake autorisasjonsmekanismer. Et eksempel kunne være et eldre, klinisk fagsystem med liten eller ingen autorisasjonskontroll, der virksomhetens retningslinjer går ut på at systemet kun skal brukes til bestemte oppgaver. En databruker som av rene bekvemmelighetshensyn gjør et oppslag i dette fagsystemet, kan da ha omgått den interne retningslinjen selv om hensikten ikke var annet enn å utføre en berettiget handling som egentlig skulle ha vært utført i et annet IT-system.

I gråsonen mellom type B3 og type C i figuren finner man overtredelser av sikkerhetstiltak som er av en slik karakter at det blir svært vanskelig å spore handlingen for å etterprøve om tilgangen har vært berettiget. Et eksempel kan være at databrukeren velger å bruke et IT-system der en annen person har logget seg på, fordi han selv mangler de tilgangene som han mener at han har behov for.

Overtredelser, både av type A og type B, forekommer i praksis i et så stort omfang at etterprøving er en betydelig oppgave.[767] Med de metodene for å undersøke og avdekke mulige overtredelser som hittil er utbredt i praksis, er imidlertid effektiv etterprøving stort sett begrenset til overtredelser av typene B1 og B2. Disse to typene er imidlertid de minst alvorlige, ettersom databrukerne nødvendigvis er oppmerksomme på at handlingene registreres og

[767] Ulike sider ved praksis er belyst i kapittel 7 ovenfor.

er sporbare. Det er også disse to typene som står for det største volumet. De øvrige typene overtredelser, A1, A2 og B3, foregår generelt under mindre oppdagelsesrisiko. I den grad slike handlinger avdekkes er det, i hvert fall hittil, i større grad resultat av at en konkret mistanke forfølges enn av systematisk undersøkelsesvirksomhet.

9 Vurdering av autorisasjonsprinsipper

I dette kapitlet presenteres og vurderes tretten forskjellige autorisasjonsprinsipper. Disse tretten prinsippene er idealtyper, og basert på begreper og ideer som til dels finnes i praktisk bruk, og til dels har vært foreslått i ulike teoretiske bidrag og faglig-politiske forslag om kontroll med tilgang til helseopplysninger. Autorisasjonsprinsippene er altså ikke «funnet opp» i arbeidet med avhandlingen. De er enten lånt direkte, eller abstrahert, fra andre kilder. Det er systematiseringen og vurderingen som er det originale bidraget her. Begrepsbruken knyttet til autorisasjonsprinsipper bygger videre på den generelle redegjørelsen for tilgangskontroll som teknologisk disiplin, i kapittel 2.3 ovenfor.

Det første underkapitlet her presenterer fire forskjellige autorisasjonsprinsipper. Disse prinsippene er utbredt i praksis, og de er generelle i den forstand at de er i bruk på mange andre områder enn bare kontroll med tilgang til helseopplysninger. De neste tre underkapitlene presenterer to autorisasjonsprinsipper hver. Det er henholdsvis to aktualiseringsmekanismer, to prinsipper for forløpsbasert tilgang, og to prinsipper for å styrke pasientens kontroll med tilgangene. Aktualiseringsmekanismene har relativt stor praktisk utbredelse innen spesialisthelsetjenesten, mens de etterfølgende fire autorisasjonsprinsippene i hovedsak fremdeles er på tegnebrettet eller under utprøving i mer begrenset målestokk. Deretter følger et underkapittel som presenterer og vurderer tre alternative modeller.

Til slutt i kapitlet er de tretten prinsippene stilt opp i en samlet tabell, men en forenklet «karaktergivning» for hvert av de fem vurderingskriteriene som er oppstilt i forrige kapittel.

9.1 Generelle og utbredte autorisasjonsprinsipper

De første fire autorisasjonsprinsippene kan betegnes som relativt konvensjonelle, i den forstand at de eksisterer i praktisk bruk, og ikke er spesielt utviklet for helsesektorens behov. De fire prinsippene kan utledes av en matrise med to dimensjoner. En dimensjon er skillet

mellom virksomhetsstyrt, sentralisert tilgangskontroll, og delegerbar tilgangskontroll der den databrukeren som produserer opplysningene styrer tilganger og eventuell videre delegerbarhet.[768] Grunnleggende sett er den sentraliserte kontrollen mer statisk, mens den delegerbare er mer dynamisk. Den andre dimensjonen dreier seg om hvorvidt tilgangene tildeles hver enkelt databruker individuelt, altså en direkte tilgang til de aktuelle objektene, eller om tilgangene tildeles til en rolle eller eventuelt en annen gruppering av databrukere, altså en indirekte tilgang via en representasjon av visse fellestrekk ved databrukerne. Illustrasjonen under viser hvordan de to dimensjonene spenner ut de fire første autorisasjonsprinsippene.

	Direkte tilgang	Indirekte tilgang
Sentralisert kontroll	1	2
Delegerbare tilganger	3	4

Figur 10 De fire første autorisasjonsprinsippene

9.1.1 Direkte tilgang, sentralisert kontroll

Dette autorisasjonsprinsippet går ut på at virksomheten bestemmer og administrerer hvilke tilganger hver enkelt databruker skal ha. Databrukeren har da prinsipielt sett ikke selv noen innflytelse over tilgangskriteriene. En forutsetning for at dette autorisasjonsprinsippet skal fungere, er at de som administrerer tilganger i virksomheten skaffer seg tilstrekkelig kunnskap om hver enkelt databrukers arbeidsoppgaver.

Ettersom tilgangskriteriene består av direkte koblinger mellom databrukeren og informasjonselementene, har virksomheten gode muligheter for å tilpasse tilgangene forholdsvis presist til det som er nødvendig for vedkommendes arbeid. To sykepleiere ved samme post trenger ikke nødvendigvis ha helt identiske tilganger. Dette autorisasjonsprinsippet skårer derfor relativt godt på kriteriet operasjonaliserbarhet innen virksomheten. Det gir imidlertid svært lite støtte for å formidle en virksomhets tilgangsvurderinger til en annen, samarbeidende virksomhet. Den avgivende virksomhets egne tilgangskriterier er basert på konkret kunnskap om sine ansattes oppgaver, og ikke på generaliseringer av egenskaper som er felles for flere databrukere, eller felles for bestemte typer oppgaver.

Muligheten for å avgrense tilgangene individuelt for hver enkelt ansatt bidrar til en viss grad også positivt til å kunne avbilde bestemmelser om taushetsplikt. Den sentraliserte

[768] Disse to grunnleggende forskjellige tildelingsprinsippene, i faglitteraturen omtalt som henholdsvis MAC (Mandatory Access Control) og DAC (Discretionary Access Control), er introdusert i kapittel 2.3.4. ovenfor.

tildelingen, som etter idealtypen ikke involverer databrukerens skjønn, er imidlertid statisk. Derfor er det lite rom for å kunne få tilgang selv eller videreformidle opplysninger til andre i spesielle situasjoner som ikke virksomheten har åpnet for på forhånd. Samsvar med bestemmelser om taushetsplikt er derfor vanskelig å oppnå, i de tilfellene der et unntak fra taushetsplikten beror på helt konkrete omstendigheter i den enkelte situasjon. Det vil enten være behov for svært hyppige endringer av tilgangskriteriene, eller for å supplere autorisasjonsprinsippet med ordninger for selvautorisering.

Visse former for medinnflytelse, som sperring av journal eller en pasients ønske om å bestemme hvilke enkeltpersoner som ikke skal få tilgang, egner dette autorisasjonsprinsippet seg godt for. Virksomheten kan håndtere disse ønskene direkte ved å trekke tilbake de aktuelle tilgangene for bestemte databrukere. Pasientens medinnflytelse behøver da ikke å være ontologisk representert i tilgangskontrollmekanismen. Pasientens rett til fornyet vurdering vil også kunne håndteres ved å tildele, for det tidsrom som er nødvendig, direkte tilgang for den som får oppgaven.

En fordel ved et relativt presist oppsett av statiske tilganger er at det begrenser databrukerens mulighet for overtredelser av type A i taksonomien. Dersom det legges grundig arbeid i å bestemme den enkeltes direkte tilganger, vil problemet med for vid praktisk tilgangsmulighet bli beskjedent. Manglende tilrettelagte mekanismer for selvautorisering fra virksomhetens side fører til at det heller ikke er aktuelt med handlinger i kategoriene B1 eller B2. Databrukerens alternativer blir da enten å mangle tilstrekkelige opplysninger når arbeidet utføres, eller å begå overtredelser av typen B3 i taksonomien. Type B3 er brudd på sikkerhetstiltak for å utføre en handling som i utgangspunktet, dersom man ser bort fra sikkerhetstiltakene, ville ha vært berettiget. Anledningen til å begå overtredelser er relativt beskjeden, men de overtredelsene som eventuelt utføres kan være vanskelige å avdekke, fordi de ikke følger et tilrettelagt og virksomhetsstyrt opplegg for overstyring av tilgangsbegrensninger.

Tilgangskontrollmekanismer som er basert på dette autorisasjonsprinsippet har generelt lav sikkerhetsfaglig anseelse. De er utbredt i praksis, men finnes kanskje først og fremst i enklere «hjemmelagde» IT-systemer i små brukermiljøer.

Dette autorisasjonsprinsippet egner seg først og fremst i relativt små virksomheter, med få databrukere, der databrukerne i liten grad har sammenfallende oppgaver. Hovedproblemene er uoversiktlige og lite standardiserte tilgangskriterier, tung administrasjon, og lite teknologisk støtte for kontroll med opplysningene når tilganger gis til databrukere i andre virksomheter.

9.1.2 Indirekte tilgang, sentralisert kontroll

Indirekte tilgang går ut på at virksomheten bygger en representasjon av tilgangskriteriene som i utgangspunktet ikke er personavhengig. Deretter gir virksomheten databrukerne tilgang ved å melde dem inn i de representasjonene av fullmaktsforhold som stemmer best overens med jobben de skal gjøre. Det mest utbredte og gjennomarbeidede begrepsapparatet for indirekte tilgang er rollebasert tilgangskontroll.[769] Rollebasert tilgangskontroll er administrasjonsvennlig, særlig for større virksomheter. Til forskjell fra direkte tilganger trenger ikke de som administrerer tilangene konkrete kunnskaper om detaljer i den enkelte databrukers arbeidsoppgaver. Personer er utbyttbare, det er tilstrekkelig å kjenne vedkommendes plass i virksomheten og organisatoriske fullmakter. Utformingen av de tillatelsene en rolle skal ha, er adskilt fra kunnskapen om hvem som skal ha disse tillatelsene. I en rollebasert tilgangskontroll kan det også legges opp til å uttrykke avhengigheter og restriksjoner mellom roller, for eksempel slik at to forskjellige roller kan være gjensidig utelukkende. I andre tilfeller kan en nærmest motsatt restriksjon være relevant, at en bestemt rolle skal omfatte alle tillatelsene fra en eller flere andre roller.

Indirekte tilgang gir virksomheter en mulighet for å arbeide med tilgangskriteriene på et abstraksjonsnivå som passer for virksomhetens størrelse og art. Det gir derfor også større virksomheter et godt utgangspunkt for å operasjonalisere tilgangskriteriene slik at de stemmer rimelig greit overens med det en gruppe databrukere har behov for i arbeidet. Presisjonsnivået er nødvendigvis noe lavere enn ved direkte tilganger, men det kan også ligge en gevinst i at tilgangskriteriene må gis en mer strukturert og mindre personavhengig utforming.

Ettersom virksomheten utfører et arbeid for å utforme generelle, strukturerte tilgangskriterier, vil det også være større muligheter for en viss klebrighet, slik at kriteriene overføres sammen med opplysningene til en mottakende virksomhet. En kontroll med opplysninger som også har effekt hos den mottakende virksomheten krever imidlertid at det foregår en betydelig samordning mellom avgiver og mottaker for å sikre at de fullmaktene som en rolle representerer er sammenlignbare. Dette autorisasjonsprinsippet tilbyr altså bare kontroll på tvers av virksomhetsgrenser så lenge tilganger deles mellom kjente aktører som samarbeider om hvordan tilgangskriteriene skal forstås.

[769] Rollebasert tilgangskontroll vokste frem som pragmatisk begrep fra 1970-tallet, men ble formalisert og gjenstand for mer vitenskapelig interesse på 1990-tallet. Standardartikkelen, som stadig siteres i sammenhenger som dette, er Ravi S. Sandhu m. fl. (1996): «Role-based access control models». I: *IEEE computer,* s. 38–47. Et begrep om databrukerens roller er også til stede, men i lite nyansert form, i *sikkerhetsnormen*.

Indirekte tilgang og sentralisert kontroll er lite egnet for å avbilde bestemmelser om taushetsplikt og om unntak fra taushetsplikten. Med konvensjonell rollebasert tilgang i en større virksomhet kommer man ikke riktig ned til det detaljplanet som helsepersonells individuelle taushetsplikt forutsetter.

En pasients ønske om medinnflytelse over behandlingen av opplysninger har i utgangspunktet ikke noen naturlig plass i rollebasert tilgangskontroll. Man kan legge opp til egne representasjoner av sperring av journal, som gjøres generelt gjeldende for databrukerne. Dersom tilgangskontrollen skal kunne håndtere spesielle tilfeller som fornyet vurdering eller en pasients ønske om at enkeltpersoner blant databrukerne ikke skal ha tilgang, krever det en egen måte å representere disse ønskene på, som bryter med prinsippet om indirekte tilganger.

Rollebasert tilgang i store enheter, der mange personer kan tildeles likeartede oppgaver overfor samme pasientgruppe, fører i utgangspunktet til at tilgangene blir vide. Det innebærer en fare for at det kan forekomme svært mange handlinger som er overtredelser av type A, både snoking og urettmessig videreformidling. Dersom tilgangene er vide, vil man mer sjelden havne i den situasjon at man mangler den praktiske tilgangen til å utføre en berettiget handling, som er overtredelser av type B. For rollebasert tilgangskontroll vil det i prinsippet være slik at forsøk på å minske felt A i overtredelsestaksonomien vil føre til at felt B utvides, og vice versa. Et stort felt A i overtredelsestaksonomien gjør det vanskelig å få oversikt over, og å avdekke, bevisste brudd på reglene.

Rollebasert tilgangskontroll er svært utbredt i praksis, og har en posisjon som teknologisk «state of the art». Det er et autorisasjonsprinsipp som fungerer effektivt i store virksomheter. Hvis arbeidet med å uttrykke kriterier er godt utført, blir resultatet oversiktlige og stringente tilgangskriterier. Det største problemet med rollebasert tilgangskontroll for helseopplysninger er imidlertid at rollene bare representerer organisatoriske fullmaktsforhold, de gir lite rom for å avbilde gjeldende bestemmelser om taushetsplikt.

9.1.3 Direkte og delegerbare tilganger

Delegerbare tilganger har som utgangspunkt at den som produserer opplysningene, eller på annet vis tilkjennes status som «eier» av opplysningene, etter eget skjønn bestemmer hvem som skal få tilgang.[770] I en del tilfeller vil en mottaker også kunne tildeles muligheten til å delegere tilgangen videre.

[770] Begreper om eierskap til helseopplysninger er problematisert i kapittel 6.1.3 ovenfor. I denne sammenhengen får det passere som en metafor for en delegasjonsadgang innen en tilgangskontrollmekanisme.

Dette autorisasjonsprinsippet er i liten grad noe man finner i robuste fagsystemer, annet enn som godt innrammede funksjoner for å overføre opplysninger til andre aktører. Databrukere vil som regel ha mer kjennskap til dette autorisasjonsprinsippet gjennom kontorstøtteprogramvare, som tekstbehandling og e-post og lignende, der man primært behandler ustrukturert informasjon. Direkte og delegerbare tilganger er vanligst i slike åpne samhandlingskanaler. Det kan imidlertid være prinsipielt mulig også å ta i bruk et slikt autorisasjonsprinsipp i behandlingsrettede helseregistre.

Virksomhetens befatning med delegerbare tilganger vil være å sette rammer for hvordan ansatte skal kunne delegere tilgang til andre. Slike rammer kan både bestå av organisatoriske bestemmelser, og av teknologisk tilrettelegging av måter å gi tilgang på. Likevel innebærer dette autorisasjonsprinsippet at virksomheten frasier seg muligheten for en uttømmende kontroll over hvem som på et gitt tidspunkt kan ha tilgang til hva.

Dette er et vesentlig mer dynamisk autorisasjonsprinsipp enn de sentraliserte, virksomhetskontrollerte prinsippene. Så langt databrukeren etterlever regelverket, gir dette prinsippet rike muligheter for å sørge for at tilganger som gis er i samsvar med bestemmelser om taushetsplikt. Problemet er imidlertid at det er opp til den databrukeren som har delegasjonsmuligheten, og ikke virksomheten, å sørge for at tilgangene som gis er berettigede. Delegerbare tilganger fungerer i prinsippet like greit over virksomhetsgrenser som innenfor en virksomhet. Det problemet virksomheten har med å etterprøve tilgangene blir imidlertid overført til alle mottakende virksomheter.

Ettersom det dreier seg om direkte tilganger, er det også her relativt gode muligheter for å tilpasse tilgangene til pasienters ønsker om medinnflytelse. Problemet med virksomhetens manglende kontroll gjør seg imidlertid gjeldende også her. Virksomheten har små muligheter for å kontrollere om pasientens ønsker blir tatt hensyn til.

Så lenge den databrukeren som gir tilgang utøver godt skjønn, og ikke begår feil, vil det bare være unntaksvis at det forekommer overtredelser i taksonomiens felt A eller B. Problemet er imidlertid at virksomheten har små muligheter for å etterprøve praksisen. Dette autorisasjonsprinsippet vil kanskje særlig være sårbart for manglende kunnskaper, systematiske misforståelser eller utglidninger over tid i databrukernes holdninger.

9.1.4 Indirekte og delegerbare tilganger

Indirekte og delegerbare tilganger er en slags hybrid, i den forstand at virksomheten kan legge relativt strenge teknologiske føringer for hvordan databrukere skal kunne gi tilgang videre til

andre. Varianter av dette autorisasjonsprinsippet vil man først og fremst finne på operativsystemnivå, i tilgangskontrollen til filkataloger og andre delte systemressurser. Det er antakelig en sjeldenhet på applikasjons- og fagsystemnivået. Dette autorisasjonsprinsippet har altså liten praktisk relevans for kontroll med tilgang til helseopplysninger. Det er med her først og fremst for å fylle ut en plass i systematikken for disse vurderingene.

At tilgangene er indirekte, gir virksomheter et godt utgangspunkt for å operasjonalisere tilgangskriteriene på en strukturert måte. Denne siden ved autorisasjonsprinsippet er i stor grad sammenlignbar med den rollebaserte tilgangskontrollen som helt og holdent styres av virksomheten. Operasjonaliseringen dreier seg om i hvilken grad virksomheten velger å overlate delegering av tilgang til den enkelte databruker. I samme utstrekning som databrukeren stilles fritt, mister virksomheten den samlede kontrollen med hvilke tilganger som gis.

Hvor godt tilgangene kan være i samsvar med gjeldende bestemmelser om taushetsplikt, vil også bero på hvilken grad av handlefrihet databrukeren får. Autorisasjonsprinsippet er dynamisk i samme utstrekning om virksomheten frasier seg kontrollmuligheter. Det er derfor et prinsipp som tilbyr en balansering mellom operasjonalisering og avbildning. Den enkelte databruker, som kan delegere tilgang, vil imidlertid ha vanskelig for å vite nøyaktig hva slags tilgang en mottaker egentlig får, ettersom mottakerens tilgang også beror på hvilke fullmakter vedkommende har fra virksomhetens side. Dette problemet har ikke databrukeren ved direkte og delegerbare tilganger. Tilgang på tvers av virksomhetsgrenser oppnår man i den utstrekning databrukeren gis handlefrihet til å delegere tilgang. Det vil imidlertid kunne være svært vanskelig å oppnå noen kontroll med hvilke rammer for den videre delegeringen av tilgangen som er etablert hos en mottakende virksomhet.

Pasienters medinnflytelse kommer ikke spesielt godt ut i dette autorisasjonsprinsippet. Det vil lide både under problemet med at tilgangen er indirekte, og derfor vanskelig kan representere ønsker som gjelder den enkelte databrukers tilgang, og problemet med delegerbarhet som fører til at virksomheten har små muligheter for å kontrollere om pasientens ønsker blir tatt hensyn til.

En fordel med dette prinsippet er at muligheten for å kombinere virksomhetenes operasjonalisering med et nærmere avgrenset handlingsrom for databrukeren bidrar til at både felt A og felt B i overtredelsestaksonomien kan holdes relativt små. Virksomheten kan unngå å gi så vide generelle tilganger at faren for snoking og uberettiget tilgang blir uforholdsmessig høy, samtidig som databrukernes anledning til å styre tilgangene selv innen gitte rammer bidrar til at man sjelden vil mangle praktisk tilgang til de opplysningene man har behov for tilgang til. Selv om dette autorisasjonsprinsippet begrenser faren for overtredelser, vil man

likevel ha et betydelig problem i at det er vanskelig å etterprøve om et regelbrudd har funnet sted.

9.2 Aktualiseringsmekanismer

Aktualiseringsmekanismer er et pragmatisk tiltak for å oppnå dynamisk og situasjonstilpasset tilgang. Kjernen i prinsippet er en selvautorisering, der databrukeren kan gi seg selv tilgang innenfor rammer som er tilrettelagt av virksomheten. Databrukeren angir sin begrunnelse for at vedkommende har behov for tilgang, og virksomheten følger opp praksisen systematisk. Det finnes flere varianter av slike aktualiseringsmekanismer, som er i praktisk bruk. Her presenteres og vurderes to idealtyper: Merking av aktive pasientrelasjoner som eksempel på en «svak» aktualiseringsmekanisme, og nødrettstilgang som eksempel på en «sterk» mekanisme. Ideen bak en svak aktualisering kan sies å være at det primært er virksomhetens måte å unngå for vide generelle tilganger på. En sterk aktualisering ivaretar helsepersonellets individuelle ansvar, og gir databrukeren anledning til å overstyre de begrensningene virksomheten har satt. Disse to autorisasjonsprinsippene har imidlertid ikke skarpe grenser mellom seg, de blandes ofte sammen, og det kan diskuteres om forskjellen egentlig er signifikant.

En viss praktisk forskjell er det likevel, ved at bruken av ulike aktualiseringsmekanismer havner i forskjellige logger, og ikke nødvendigvis er gjenstand for samme grad av oppfølging fra virksomheten.[771] Svak aktualisering er plassert i feltet B1 i overtredelsestaksonomien, mens sterk aktualisering er plassert i feltet B2.

9.2.1 Merking av aktive pasientrelasjoner

For at ikke opplysninger om en pasient skal kunne være tilgjengelig til enhver tid, for alle som har tilgang etter ordinære kriterier, vil det i mange tilfeller være slik at en tilgang beror på at det blir merket av om en pasientrelasjon for tiden er aktiv. En pasientrelasjon er for tiden aktiv når vedkommende pasient faktisk er inne til undersøkelse eller behandling. Det kan også være hensiktsmessig å holde relasjonen aktiv en kort periode etter utskriving, for å håndtere etterarbeid og mulige henvendelser. Ny aktualisering kan være nødvendig for eksempel ved en senere telefonhenvendelse fra pasienten. Det kan både være behandlende helsepersonell og de som arbeider i pasientadministrative funksjoner som har behov for tilgang mens en

[771] I følge sikkerhetsnormen skal nødrettstilganger behandles som avvik, noe som innebærer at de skal følges opp enkeltvis. En så streng føring gjøres vanligvis ikke gjeldende for svakere aktualiseringsmekanismer.

pasientrelasjon er aktiv. Vanligvis blir dette gjennomført ved at databrukeren velger blant et oppsett av standardiserte begrunnelser for at tilgangsbehovet. En metafor som av og til brukes om slike funksjoner er «grønnlystilganger». Dette er en mekanisme som er utbredt blant de markedsledende EPJ-systemene i sykehussektoren. Mange, men ikke alle, virksomheter har tatt den i bruk.

Virksomheter som tilrettelegger for en slik aktualiseringsmekanisme gjør det som en tilleggsrestriksjon til andre måter å operasjonalisere tilganger på, som regel som en utvidelse av rollebasert tilgangskontroll. Hovedpoenget er å unngå for vide generelle tilganger, slik at man derved reduserer omfanget av felt A i overtredelsestaksonomien. I stedet får man en tilsvarende økning av hendelser som havner i taksonomiens felt B1, noe som i utgangspunktet er en styrt kanalisering. Tilganger som fanges opp i felt B1 kan undersøkes nærmere, og dersom en begrunnelse ikke er tilstrekkelig plausibel kan det gi grunn til en mistanke om snoking eller et brudd på taushetsplikten.

Så langt virksomheten lykkes i å følge opp tvilsom bruk av aktualiseringsmekanismen, vil den skåre godt på samsvar med bestemmelser om taushetsplikt.

Pasientens medinnflytelse ivaretas i det store og hele ikke på en overbevisende måte ved aktualisering. Først og fremst må en medinnflytelse innebære begrensninger i hva det er mulig å overstyre gjennom aktualisering. Det er for eksempel lite betryggende for pasienten om en databruker kan bruke aktualisering for å komme inn i en sperret journal. For å ivareta pasientens ønske om å detaljstyre hvilke databrukere som skal eller ikke skal ha tilgang, må slike former for medinnflytelse representeres eksplisitt, og fortrinnsvis ha høyere rang enn aktualiseringsmekanismen.

En aktualisering gir svært lite rom for sammenhengende kontroll på tvers av virksomhetsgrenser. Merkingen av at pasienten er aktiv, og den konkrete vurderingen av behovet for tilgang, kan nærmest per definisjon bare ha gyldighet for den virksomheten der aktualiseringen har oppstått. Dersom man skulle se for seg at merking av en aktiv pasientrelasjon er klebrig, for også å gjelde i en samarbeidende virksomhet, vil det i realiteten ikke lenger være en aktualisering. En slik situasjon vil ligne mer på en beslutningsstyrt tilgang, med andre krav til etterrettelig dokumentasjon av grunnlaget for tilgang. Beslutningsstyrt tilgangskontroll er et av de andre autorisasjonsprinsippene som er vurdert nedenfor.

Samlet sett kan man si at en aktualiseringsmekanisme er et pragmatisk og hensiktsmessig instrument for å balansere virksomhetens operasjonalisering mot avbildning av bestemmelser om taushetsplikt. Virksomheten beholder en relativt høy grad av kontroll ved å tilrettelegge for målrettet og strukturert etterhåndskontroll. Aktualisering fører imidlertid med seg to store

problemer. Det ene er at aktualiseringer kan «kveles i sin egen suksess», ved at volumet av tilfeller som trenger oppfølging blir altfor stort til at etterprøvbarheten blir reell. Det andre problemet, som kanskje er enda mer diskvalifiserende i lys av denne avhandlingens tema, er at aktualiseringer ikke egner seg for meningsfull kontroll på tvers av virksomhetsgrenser.

9.2.2 Nødrettstilganger

Nødrettstilganger er det enkelte helsepersonells individuelle adgang til å overstyre tilgangsbegrensninger.[772] Til forskjell fra merking av aktiv pasientrelasjon, skal begrunnelse for at det er behov for tilgang som regel angis i fritekst. Det kan ses i sammenheng med ideen bak en slik sterkere aktualiseringsmekanisme, det bør være mer spesifikke grunner til at tilgangen er nødvendig for akkurat denne databrukeren enn det som angis sjablongmessig gjennom en standardisert tekst. I praksis viser det seg imidlertid at fritekstfeltet ofte fylles ut med standardfraser som «helsehjelp» og lignende, uten at det legges mye arbeid i å konkretisere begrunnelsen.[773] En metafor som av og til brukes om nødrettstilganger er «blålystilgang».

Bruk av en nødrettstilgang er prinsipielt legitimert gjennom profesjonsutøverens subjektive faglige skjønn, og skal følges opp ved at hver enkelt tilgang behandles som et avvik. Slike tilganger hører hjemme i kategori B2 i overtredelsestaksonomien. Selv om grunnlaget for å bruke en sterk aktualiseringsmekanisme er noe annerledes enn for en svakere mekanisme, og det forutsettes en tettere oppfølging, er forskjellen likevel ikke særlig stor i praksis.

I det store og det hele blir resultatet av vurderingen av dette autorisasjonsprinsippet det samme som for svakere aktualiseringsmekanismer. Nødrettstilganger skårer imidlertid noe høyere på samsvar med bestemmelser om taushetsplikt, fordi det forutsetter en mer subjektiv vurdering direkte fra helsepersonell som er pliktsubjekt i den aktuelle situasjonen.

9.3 Forløpsbasert autorisasjon

En annen strategi for å gjøre tilgangskontrollen mer dynamisk er å la behovet for tilgang følge av bestemte handlinger og hendelser under den enkelte pasientens behandlingsforløp. Mens aktualisering går ut på at behovet for tilgang vurderes subjektivt av den som har behov for

[772] Selv om betegnelsen «nødrettstilgang» kan være litt tvilsom, har dette behovet for at helsepersonell skal kunne overstyre virksomhetens fastlagte begrensninger lang historie som helserettslig tema, jf. drøftingen i kapittel 6.4.2.4 ovenfor.
[773] Jf. kapittel 7.3.2.3 ovenfor.

tilgangen, vil forløpsbasert autorisasjon i større grad innebære at muligheten for tilgang oppstår og forsvinner igjen når opplysninger om behandlingsforløpet tilsier at behovet er der.

Også her er det hensiktsmessig å presentere to idealtypiske varianter, selv om man i praksis kunne se for seg mellomløsninger mellom disse. Den ene varianten kan kalles beslutningsstyrt tilgangskontroll, og går ut på at registreringen av en behandlingsbeslutning, for eksempel en henvisning, behov for å avlegge en bestemt prøve, pasientens ønske om å velge et bestemt sykehus, med videre, åpner tilgangen for de som skal utføre det som beslutningen gjelder. En beslutning eller hendelse kan også tilsi at noen som tidligere hadde tilgang ikke lenger vil ha bruk for den. Beslutningene som berettiger tilgang treffes av den aktuelle behandler, når situasjonen tilsier det. Det er dermed en skjønnsbasert tilgangskontroll, som ikke reguleres uttømmende fra virksomhetens side.[774]

Den andre idealtypiske varianten baserer tilgangene på forhåndsdefinerte oppsett av behandlingsprosesser. Tilgangene styres da ut fra kriterier som virksomheten har utformet, basert på medisinskfaglige veiledninger og standarder for hvordan et medisinsk problem hos en pasient bør håndteres. Hvis for eksempel et bestemt symptom eller en diagnose tilsier en bestemt sekvens av undersøkelser og behandlinger, kan tilganger åpnes og stenges automatisk ut fra den sjablongmessig definerte prosessen. I praksis vil man antakelig trenge noe større fleksibilitet enn denne skisserte idealtypen, men så langt man holder seg til den vil dette være et autorisasjonsprinsipp som virksomheten har full kontroll med.[775]

9.3.1 Beslutningsstyrt tilgangskontroll

Autorisasjonsprinsippet går ut på at tilgang knyttes til beslutninger som gjelder behandling av pasienten.[776] I utgangspunktet treffes det en rekke ulike typer beslutninger innen et behandlingsforløp. Mange beslutninger overfører oppgaver til andre, slik som henvisninger, innleggelser, prøvebestillinger, resepter med videre. Andre beslutninger gjelder handlinger som den som treffer beslutningen gjennomfører selv. Beslutningsbegrepet i denne sammenhengen dreier seg ikke først og fremst om å treffe vedtak, i den betydningen at det er et spørsmål med en tydelig initiering som skal vurderes og gis et begrunnet svar. Beslutninger kan også være ulike mellomliggende handlinger i en sammensatt utredning eller behandling. Man kan

[774] Det er dermed en variant av det ene teoretiske begrepet for tildeling av tilganger, Discretionary Access Control, «DAC», jf. kapittel 2.3.4 ovenfor.
[775] Det er dermed en variant av Mandatory Access Control, «MAC», jf. kapittel 2.3.4 ovenfor.
[776] Beslutningsstyrt tilgang er beskrevet i Nystadnes (2007b), riktignok i en variant som ligger nærmere en mellomting mellom de to idealtypene beslutningsstyrt og basert på definerte behandlingsopplegg som er beskrevet her. Et krav til å basere tilgang på beslutninger finnes også i sikkerhetsnormen s. 16.

kanskje heller se dette beslutningsbegrepet i sammenheng med helsepersonells dokumentasjonsplikt, handlinger må dokumenteres hvis dokumentasjonen kan bli nødvendig.[777]

Det er imidlertid likevel grenser for hvor langt det er rimelig å strekke begrepet beslutning. Hvis for eksempel en pårørende ringer for å få vite noe, og behandleren er berettiget til å svare på spørsmålet, vil man antakelig tøye begrepet dersom det å svare på spørsmålet ses som en beslutning knyttet til behandlingsforløpet. Det er mer nærliggende å tenke i retning av aktualisering i slike situasjoner. Det at ikke «alt er beslutninger» peker også mot noe av det som kan være en svakhet ved dette autorisasjonsprinsippet. Dersom det finnes reelle behov for tilgang, uten at noen eksisterende beslutninger utløser denne tilgangen, kan man ende opp med å konstruere kunstige beslutningspunkter for å tilfredsstille tilgangskriterier.[778] Andre problemer som man kan støte på med en slik tilgangsmodell er at det må kunne stilles høye krav til datakvaliteten i helseopplysningene for at en beslutning skal resultere i tilganger som både er berettigede og som er i samsvar med behovene.

Virksomhetens operasjonalisering, og ansvaret for å sørge for at tilgang bare gis i den grad dette er nødvendig for vedkommendes arbeid, utøves først og fremst i tilretteleggingen av hvilke beslutningspunkter som skal utløse hvilke tilganger. Det innebærer at en relativt stor del av kontrollen med tilgangene blir liggende på virksomheten. Likevel er det gjennom den praktiske pasientbehandlingen, der beslutninger treffes og dokumenteres, at konkrete tilganger oppstår eller forsvinner. Dermed har ikke virksomheten fullt ut uttømmende kontroll over tilganger, men man kan likevel oppnå bedre treffsikkerhet i praksis enn for eksempel ved en rendyrket rollebasert tilgangskontroll.

Autorisasjonsprinsippet vil være godt egnet til å oppfylle krav til samsvar med bestemmelser om taushetsplikt. De beslutninger som en behandler treffer, og som overfører oppgaver til andre, vil i utgangspunktet være innenfor vedkommendes opplysningsrett i den grad virksomheten har lykkes med en holdbar operasjonalisering av tilgangskriteriene. Opplysningsretten som gir anledning til å gi opplysninger til samarbeidende helsepersonell er basert på et implisitt samtykke, slik at pasienten har en innsigelsesrett.[779] I de fleste tilfeller vil en slik inn-

[777] I mange slike tilfeller er dokumentasjonen det som kan kalles et performativ, for eksempel er en henvisning en dokumentasjon som «gjør det den sier». Jf. John Langshaw Austin (1962): *How to do things with words*.
[778] I en rapport fra en workshop, mellom flere virksomheter og premissgivende aktører, ble problemet med manglende beslutningspunkter beskrevet som et problem: «Rikshospitalet har prøvd ut denne tankegangen med 'hendelsesbasert' tilgangsstyring, og har blant annet brukt en innkommet henvisning som en hendelse som brukes for å gi helsepersonell tilgang til helseopplysninger. En utfordring er at det til nå ikke er mange slike definerte tiltak som kan brukes som basis for tilgangsstyring.» Bjarte Aksnes og Magnus Alsaker (2005): «Elektronisk tilgang til helseopplysninger – utfordringer og mulige tiltak», s. 13.
[779] Helsepersonelloven §§ 25 og 45.

sigelse antakelig ha form av en innsigelse mot den bakenforliggende beslutningen, for eksempel at pasienten ikke ønsker å gjennomføre en bestemt undersøkelse, eller motsetter seg en bestemt type behandling. Pasienten kan imidlertid også kreve, innenfor det som er praktisk mulig, at visse opplysninger holdes tilbake fra samarbeidende helsepersonell uten å motsette seg selve behandlingen. En slik situasjon vil forutsette egne representasjoner av pasientens ønsker, som virksomheten tar hensyn til når de utarbeider koblingene mellom beslutningstyper og tilgangskriterier. Generelt vil det være tungvint, men mulig, å tilrettelegge en tilgangsmekanisme basert på dette autorisasjonsprinsippet for pasienters medinnflytelse. Et ønske fra pasienten om fornyet vurdering er imidlertid en form for medinnflytelse som dette prinsippet er svært godt egnet for.

Beslutningsstyrt tilgangskontroll egner seg godt for klebrige tilgangskriterier, som kan flyte forholdsvis fritt over virksomhetsgrenser. Det krever imidlertid, i likhet med rollebasert tilgang, at virksomhetene samarbeider om hvordan koblingen mellom beslutningstyper og tilgangskriterier skal forstås i praksis. En slik felles forståelse mellom virksomheter kan være bilateral, eller basert på en mer overordnet samordning.

Både felt A og felt B i overtredelsestaksonomien kan i utgangspunktet bli små og oversiktlige med beslutningsstyrt tilgangskontroll. Dersom virksomheten har behov for stor fleksibilitet i organiseringen av arbeidet, slik at mange ulike enkeltpersoner skal kunne stille opp for å gjennomføre et gitt tiltak, vil det imidlertid føre til at felt A, faren for snoking eller brudd på taushetsplikten, også blir større.

Varianter av beslutningsstyrt tilgang finnes, dels under utprøving og dels i drift i mindre skala. Det vil imidlertid være et svært omfattende arbeid å skulle gjennomføre et slikt autorisasjonsprinsipp i bredt omfang på tvers av virksomhetsgrenser og IT-systemer.

9.3.2 Tilganger basert på definerte behandlingsopplegg

Den andre idealtypiske varianten av forløpsbasert autorisasjon er å definere sjablonger for typiske behandlingsprosesser, og så knytte tilgangsrettighetene til de som vanligvis skal samhandle i en slik prosess.[780] Å styrke tilgangsstyringen ved å ta i bruk prosessinformasjon er også antydet som en mulighet i en rapport der det anbefales å legge om selve

[780] Slike definerte behandlingsopplegg kan være innenfor en virksomhet eller mellom virksomheter, men man kan også tenke seg at generelle medisinskfaglige retningslinjer brukes om utgangspunkt for å sette opp tilgangskriterier, slik det er foreslått i Lillian Røstad (2007): «MG-RBAC: Using Medical Guidelines as a Source of Contextual Information to Activate and Deactivate Roles and Permissions» (konferanseartikkel), der informasjon om typiske behandlingsforløp kombineres med en rollebasert tilgangskontroll.

organiseringen av journalen til en mer prosessorientert, i stedet for kildeorientert, struktur.[781] Fordi autorisasjonsprinsippet er basert på sjablonger for behandlingsprosesser, og ikke på konkrete beslutninger, blir virksomhetens sentrale kontroll betydelig større enn ved beslutningsstyrt tilgangskontroll.

Tilganger basert på definerte behandlingsopplegg gir, i likhet med rollebasert tilgangskontroll, virksomheten mulighet for å legge opp gjennomarbeidede generelle tilgangskriterier. I tillegg vil presisjonsnivået kunne bli en del høyere enn for generelle roller, fordi tilgangskriteriene i mer direkte forstand representerer kunnskap om hva som er nødvendig i den enkeltes arbeid. Derfor ivaretar dette autorisasjonsprinsippet i utgangspunktet samsvaret med bestemmelser om taushetsplikt rimelig godt. Dette er imidlertid en avbildning som er på virksomhetens premisser, den gir ikke databrukeren diskresjonær adgang til å ta stilling til om et unntak fra taushetsplikten kan komme til anvendelse i en situasjon. Derfor kan denne avbildningen, selv om den skulle være relativt treffsikker, oppleves som lite fleksibel. For databrukeren vil det kunne bli vanskelig å forstå hvorfor tilgang nektes i en konkret situasjon.

I den grad tilgangskriteriene kan knyttes til generelle medisinskfaglige retningslinjer vil man også kunne oppnå felleskriterier som i høy grad sikrer at det samme kriteriet betyr det samme når det gis tilgang til opplysninger mellom virksomheter. I helt rendyrket form, vil dette autorisasjonsprinsippet kunne fungere på tvers av virksomhetsgrenser uten en direkte samordning av tilgangskriterier mellom virksomhetene.

I likhet med det som gjelder for rollebasert tilgangskontroll har pasienters ønske om medinnflytelse over behandlingen av opplysninger heller ikke her noen naturlig plass. Dersom tilgangskontrollmekanismen skal kunne ta hensyn til pasientens ønsker om å påvirke behandlingen av opplysninger, krever dette egne representasjoner og mekanismer.

Et godt opplegg for tilgang basert på definerte behandlingsprosesser fører til at felt A i overtredelsestaksonomien får et ganske beskjedent omfang. Felt B vil kunne bli en del større, fordi databrukeren mangler diskresjonære muligheter for å bestemme over tilgangene. Dermed kan det jevnlig oppstå situasjoner der en tilgang ville ha vært berettiget, men uten at databrukeren har denne tilgangen i praksis. Av den grunn er det kanskje rimelig å se for seg at dette autorisasjonsprinsippet ikke brukes alene, men helst i kombinasjon med en aktualiseringsmekanisme.

Foreløpig er tilgangskontroll basert på definerte behandlingsprosesser primært på teoristadiet. Denne tanken kan betraktes som del av en større helseinformatisk endring enn bare å

[781] Grimsmo m. fl. (2007), s. 16.

klekke ut gode tilgangskriterier. Å utvikle systematikk for prosessorganisering av helseopplysninger, med koblinger mellom faglige standarder, lokale prosedyrer og konkret pasientbehandling er et eget forskningsfelt, som antas å kunne få store følger for behandling av helseopplysninger generelt.[782] Det er først og fremst i sammenheng med en slik større endring av informasjonssystemene at dette autorisasjonsprinsippet kan bli et sannsynlig og interessant scenario.

9.4 Medinnflytelsesbasert autorisasjon

I de foregående vurderingene av ulike autorisasjonsprinsipper kom pasientens medinnflytelse over opplysningene i de fleste tilfeller ut som et mer eller mindre brysomt element. Det er et hensyn som er lite tilgodesett i konvensjonell tilgangskontroll, og man kan nok ikke si at det har en entydig sterk posisjon i reguleringen heller. De to autorisasjonsprinsippene som følger her, snur noe om på dette. De tar begge, på hver sin måte, pasientens medinnflytelse som utgangsposisjon. Her trekkes det et skille mellom pasientstyrte tilganger og pasientholdte data. Pasientstyrt innebærer at helseopplysningene befinner seg i helsetjenestens informasjonssystem, men kontrolleres av eller på vegne av pasienten. Pasientholdte data kan befinne seg hos pasienten selv, eller hos en uavhengig tredjepart som pasienten i prinsippet står fritt til å velge selv. I praksis kan man tenke seg, og det er kanskje vel så sannsynlig, ulike mellomløsninger mellom disse autorisasjonsprinsippene.[783]

9.4.1 Pasientstyrt tilgangskontroll

Når pasienten skal kunne bestemme over tilgangene, er en forutsetning for at det skal ha særlig mening i praksis at også de helseopplysningene som pasienten administrerer tilgang til gjøres direkte tilgjengelige for pasienten. Pasientstyrt tilgangskontroll vil derfor kunne være egnet som en del av det man betegner som e-helse, og «den aktive pasient». Det dreier seg likevel om en mulighet for frivillig medinnflytelse så langt pasienten ønsker. Derfor vil en viktig del av dette autorisasjonsprinsippet dreie seg om at de grunnleggende kravene til en tilgangskontroll må innfris også når pasienten velger å være passiv.

[782] Grimsmo m. fl. (2007).

[783] En slik kombinasjon av disse autorisasjonsprinsippene er utførlig redegjort for, med en liste over noen nærmest aksiomatiske forutsetninger, i Lillian Røstad og Øystein Nytrø (2008): «Personalized access control for a personally controlled health record» (konferanseartikkel).

Virksomheten har i utgangspunktet en temmelig begrenset mulighet for å sikre at tilganger bare gis til de som har behov for opplysningene i sitt arbeid. Et visst minstemål av operasjonalisering av tilganger må virksomheten gjennomføre, men virksomhetens tilgangskriterier skal kunne overprøves av den pasienten som ønsker å gjøre det. Pasientens råderett har imidlertid en klar begrensning, pasienten har ikke anledning til å frita helsepersonell fra dokumentasjonsplikt, eller fra lovpålagte opplysningsplikter. Det er først og fremst på de områdene hvor pasienten allerede i utgangspunktet har rett til, eller kan gis anledning til, å øve medinnflytelse at dette autorisasjonsprinsippet får betydning.

Samsvaret med bestemmelser om taushetsplikt vil i utgangspunktet kunne fungere bra, fordi pasientens beslutninger om hvem som skal få tilgang vil kunne fungere som et samtykke til formidling av opplysninger.[784] I praksis kan man støte på vanskeligheter dersom for eksempel virksomheten endrer organisering, eller hvis pasienten har lagt opp til at så få personer skal kunne få tilgang at opplysningene er utilgjengelige for relevant helsepersonell når en ansatt skifter jobb eller er sykmeldt. Endringene i virksomhetens organisering skjer ikke nødvendigvis i de periodene hvor pasienten er aktiv. Han kan i prinsippet ha gjort seg flid med å treffe beslutninger om tilgang den ene uken, men uten å gjenkjenne den organiseringen han forholdt seg til uken etter. Det vil være vanskelig for virksomheten å nå frem til alle aktuelle pasienter hver gang det skjer endringer som kan påvirke den medinnflytelsen pasienten har ønsket å utøve, fordi slike endringer kan finne sted også mellom to perioder der pasienten er aktiv.

Likevel skårer dette autorisasjonsprinsippet relativt godt, både på samsvar med taushetsplikt og på pasientens medinnflytelse. I utgangspunktet kan pasientens valg også være klebrige, slik at de gjøres gjeldende når tilgang gis til andre virksomheter. Her kan imidlertid effekten være noe mer usikker. Selv om en samarbeidende virksomhet har et opplegg på plass for å håndtere pasientens ønsker, kan det være vanskelig å anskueliggjøre hvordan disse ønskene faktisk blir håndtert i den mottakende virksomheten. Selv om tilgangskriteriene fungerer etter hensikten, og etter det som er avtalt, kan det likevel være vanskelig å gi pasienten en overbevisende opplevelse av å ha kontroll med tilgangene på tvers av virksomhetsgrenser.

Når pasienten utformer kriteriene for tilgang, kan han i utgangspunktet lykkes godt med å begrense faren for overtredelser både av type A og type B i taksonomien. De ovennevnte problemene med at organisatoriske endringer, som pasienten ikke har vært kjent med, kan medføre en utilsiktet effekt på pasientens valgte tilgangskriterier, innebærer imidlertid at det

[784] Jf. helsepersonelloven § 22.

antakelig vil være nødvendig å kunne overstyre pasientens valg når det er nødvendig. En slik overstyring kan enten være at virksomheten tvinger gjennom noen minimumskriterier som ikke pasienten kan avskjære, eller en form for aktualiseringsmekanisme. Da vil man i praksis ende opp med å utvide felt B i taksonomien, muligens i strid med pasientens ønsker.

9.4.2 Pasientholdte data

Pasientholdte data er noe helsepersonelloven åpner for, under betegnelsen egenjournal.[785] Det er i utgangspunktet en gammel, og teknologiuavhengig, idé. Helsekort for gravide har man hatt i nærmere tretti år. Det har også vært foreslått at pasienten selv kan besitte helseopplysningene på et smartkort eller tilsvarende medium. Mer nylig har det dukket opp tredjeparts-alternativer, som gir pasienten en mulighet for å velge å plassere sine helseopplysninger hos en aktør som er uavhengig av de aktuelle virksomhetene i helsetjenesten.[786]

Pasientens medinnflytelse er i utgangspunktet svært godt ivaretatt når pasienten besitter opplysningene. Pasienten kan «stemme med føttene», valg av hvem man deler opplysninger med er en helt konkret handling. Det gir lite støtte for både virksomhetens operasjonalisering av tilganger og tilgangskriterier som avbilder bestemmelser om taushetsplikt, men på den annen side vil ikke disse vurderingskriteriene lenger være like relevante. Både det å sikre at opplysninger bare blir tilgjengelige for personell med tjenestelige behov og det å sikre samsvar med gjeldende regler om taushetsplikt blir i prinsippet godt ivaretatt ved at pasienten treffer valgene selv. Dette autorisasjonsprinsippet er antakelig også det som kommer nærmest å eliminere både felt A og felt B i overtredelsestaksonomien.

Hovedproblemet for dette autorisasjonsprinsippet er ikke lenger egentlig tilgangsstyringen som sådan. Det oppstår imidlertid andre, og kanskje vel så grunnleggende spørsmål som har å gjøre med virksomhetens plikter overfor pasienten, og helsepersonellets dokumentasjonsplikt. En pasient har ikke adgang til å opptre som «redaktør» over opplysninger som er dokumentert av forskjellig helsepersonell i medhold av deres dokumentasjonsplikt. En plassering av databehandlingsansvaret som fungerer både formelt og praktisk kan være vanskelig å oppnå, særlig hvis man ser for seg at et sterkt varierende antall samhandlende helsepersonell og virksomheter kan være involvert i ulike pasienters egenjournal, avhengig av den enkelte pasientens helsetilstand og preferanser.

---

[785] Helsepersonelloven § 39(3). Denne måten å organisere helseopplysninger på er også nærmere omtalt i kapittel 5.2.2.4 ovenfor.

[786] De konkurrerende kommersielle alternativene Microsoft® HealthVault og Google™ Health har foreløpig ikke stort å tilby norske pasienter, men det er en nærliggende tanke at det vil kunne endre seg etter hvert.

En innvending, som riktignok må klassifiseres som paternalistisk, er at en pasient som får fylt opp egenjournalen, og kanskje ikke lenger har evner og overskudd til å håndtere den, vil kunne komme til å handle i strid med egne interesser. En egenjournal er et prinsipp som fører til at man i stor grad blir avhengig av pasientens kunnskaper og motivasjon, og kanskje også av pasientens evne til å henge med i en faglig og teknologisk utvikling.

9.5 Alternativer til konvensjonelle modeller for autorisasjon

De første ti autorisasjonsprinsippene, som er presentert foran i dette kapitlet, kan betegnes som relativt konvensjonelle prinsipper, eller som varianter og suppleringer av konvensjonelle prinsipper for å håndtere noen av de særegne problemene for tilgang til helseopplysninger. Et grunnleggende fellestrekk er at de er basert på en representasjon av databruker, dataelement, og relasjoner mellom disse, som angir hva som tillates. Relasjonen kan være direkte mellom databruker og dataelement, eller indirekte mellom representasjoner av grupper av databrukere eller grupper av dataelementer.

De tre prinsippene som presenteres og vurderes i dette underkapitlet går, på forskjellige måter, ut over dette grunnleggende fellestrekket. Derfor kan de betegnes som alternativer til de konvensjonelle modellene. De er utviklet for å løse forskjellige typer problemer. Ingen av dem har i utgangspunktet oppstått i helseinformatikken, men alle har vært foreslått som mulige svar på det sammensatte behovet for tilgang til og beskyttelse av helseopplysninger.

9.5.1 Spesifikasjonsspråk for tilgangspolitikk

En strategi for å styre store informasjonssystemer, særlig når de er spredt over forskjellige tekniske installasjoner, er å angi regler for å styre systemets adferd. Slike regler kalles gjerne «policies», og er uttrykk for den politikk man har valgt å styre informasjonssystemet etter.[787] Denne styringsstrategien ble i utgangspunktet utviklet for distribuerte informasjonssystemer, en beslutning om hva som er tillatt og forbudt i systemet skal håndheves likt selv om det logiske systemet er fordelt på ulike fysiske systeminstallasjoner. En policy må derfor kunne fordeles til andre installasjoner som inngår i informasjonssystemet, og håndheves med samme

[787] Morris Sloman (1994): «Policy driven management for distributed systems». I: *Journal of network and Systems Management,* s. 333–360. Denne artikkelen er svært ofte henvist til som en slags teoretisk basis for en omfattende litteratur om policy management. Den gir ingen helt presis definisjon av policies, men omtaler det som «information which influences the behaviour of the system.»

semantiske mening i alle involverte installasjoner. Med terminologien som er brukt foran, kan man si at klebrighet er et av de opprinnelige formålene med formelle policyuttrykk.

Kontroll med tilgang til bestemte dataelementer er bare en begrenset del av det man kan bruke et policybasert styringssystem til. Det er imidlertid en type anvendelse som det har vært stor interesse for, og det har vært utviklet flere forskjellige spesifikasjonsspråk for å uttrykke tilgangspolitikk i tråd med disse prinsippene.[788]

Det er særlig to trekk ved dette prinsippet som er skiller det fra de mer konvensjonelle modellene for autorisasjon, og som gjør det verdt å ta med blant de prinsippene som vurderes. Det ene trekket er at det gis mulighet for å uttrykke rikere egenskaper i relasjonene mellom databruker og dataelement. I konvensjonell tilgangskontroll er alle relasjoner i prinsippet en tillatelse, selv om tillatelser kan gjelde ulike handlinger, for eksempel, søke, lese, sende, endre, slette. Et forbud er negasjonen, fraværet av en tillatelse. I spesifikasjonsspråk som skal kontrollere et systems adferd vil relasjonene derimot kunne ha flere typer normativ modalitet som representeres eksplisitt, for eksempel plikter, forbud, eller betingelser som må være innfridd for at en tillatelse skal gjelde. Både ufravikelige krav som stilles av virksomheten og adgang til å delegere tillatelser kan uttrykkes side om side i en samlet tilgangspolitikk. Reglene vil, som i konvensjonell tilgangskontroll, anvendes på de handlinger en databruker forsøker å utføre, men de kan i tillegg regulere bestemte tilstander i systemet som utløses av andre hendelser enn brukeres handlinger.[789]

Det andre trekket er et skarpt prinsipielt skille mellom policyuttrykk og gjennomtvinging. Policyuttrykkene lages og endres i en styringsenhet, adskilt fra den enheten som tvinger gjennom den til enhver tid gjeldende policy. Den enheten som tvinger policyene gjennom er det vanlig å fremstille som en todelt overvåkningsenhet, der én modul *beslutter* om tilgang gis eller ikke, mens den andre modulen sørger for å gi eller avslå den forespurte tilgangen.[790]

De rikere mulighetene for å uttrykke forskjellige slags relasjoner mellom databrukere og dataelementer, samt tilstander som skal være oppfylt i informasjonssystemet, fører til at ulike policyuttrykk kan gjelde samtidig som mulige svar på samme forespørsel om tilgang. Derfor er den beslutningen om tilgang som overvåkningsenheten skal treffe ikke nødvendigvis triviell eller opplagt. Det er behov for en strategi eller mekanisme for å kombinere de aktuelle

[788] For eksempel er policyspråket *ponder* utviklet for primært å uttrykke autorisasjonspolitikk, Nicodemos Damianou m. fl. (2001): «The ponder policy specification language» (konferanseartikkel). Et annet, som det finnes en god del litteratur om, er *xacml.* En vurdering, opp mot enkelte spesielle tilgangssituasjoner som er relevante for helseopplysninger, finnes i Felix Apitzsch m. fl. (2008): «Specifying Security Policies For Electronic Health Records» (konferanseartikkel).
[789] Jf. skillet mellom *event triggers* og *state triggers*, Bjørnar Solhaug m. fl. (2007): «Specifying Policies Using UML Sequence Diagrams – An Evaluation Based on a Case Study» (konferanseartikkel).
[790] Felix Apitzsch m. fl. (2008), s. 86.

policyuttrykkene, slik at resultatet blir et entydig svar på forespørselen. En slik strategi for å kombinere policyuttrykk kan betegnes som en metapolicy. I en del spesifikasjonsspråk er det anledning til å angi ulike varianter av hva slags kombinasjonsstrategi som skal brukes.[791] Dermed er det ganske treffende å karakterisere policybasert styring av informasjonssystemer som en form for normer. Policyuttrykkene kan ha ulike normative modaliteter, og spesifikasjonsspråket inneholder egne tolknings- og motstridsprinsipper.

Det kan være verdt å nevne et trekk ved policybasert styring av systemer som man ofte finner omtalt i litteraturen, men som ikke vektlegges her. I en del tilfeller er man opptatt av bevisbarhet, altså å kunne undersøke formelt om endringer i eller kombinasjoner av policyer faktisk gir det resultat man har ønsket.[792]

Betraktet som et autorisasjonsprinsipp vil policybasert styring være svært godt egnet for å operasjonalisere virksomhetens besluttede tilgangskriterier. Det er i hovedsak slik en policy blir til, som en sentralisert administrativ beslutning og handling. Overføring av en policy mellom virksomheter og systemer ligger det i utgangspunktet også godt til rette for, klebrighet på tvers av komponenter i et distribuert system er en stor del av bakgrunnen for dette prinsippet. Å iverksette en konkret policy i forskjellige systemer krever imidlertid en omfattende samordning av disse systemenes semantiske innhold, fordi hver policy normalt vil bli iverksatt som den er, uten å bli omformulert eller tilpasset når den anvendes i et annet IT-system.

Policybasert styring vil også kunne egne seg relativt godt til å avbilde bestemmelser om taushetsplikt. En policy kan uttrykkes svært detaljert, og det er relativt vanlig at spesifikasjonsspråk gir rom for å uttrykke delegerbare policyer.

Pasientens medinnflytelse er vanskelig å uttrykke direkte gjennom de policyer virksomheten definerer. Visse former for medinnflytelse, som sperring av journal, vil kunne ivaretas ved å etablere egne ontologiske representasjoner av de valgene pasienten gjør. Dermed kan en tilgangspolicy uttrykkes slik at den overholder de valgene pasienten har meddelt til informasjonssystemet.[793]

---

[791] For eksempel kan man i xacml-språket, som to av fire slike kombinasjonsmuligheter, angi at det skal gis avslag dersom det finnes minst én negativ policy blant flere mulige, eller at tilgang skal tillates dersom det finnes minst én positiv policy blant flere mulige.

[792] Moritz Y. Becker (2007): «Information governance in NHS's NPfIT: A case for policy specification». I: *International Journal of Medical Informatics,* s. 432–437.

[793] Et forslag til hvordan dette kan gjøres er beskrevet i Becker (2007): Pasientdatasystemene utstyres med en funksjonalitet som beskrives metaforisk som en «forseglet konvolutt». Ulike notater kan plasseres der etter ønske. Policyer uttrykker generelt forbud mot å åpne «konvolutten», og detaljerte betingelser som må være innfridd om den likevel skal åpnes.

Både muligheten for høy detaljeringsgrad i policyene og mulighetene for å uttrykke konkrete forbud og vilkår for tilgang, gjør det mulig å oppnå at både felt A og felt B i overtredelsestaksonomien holdes relativt små. Dersom en overtredelse er begått, kan likevel etterprøving være noe mer komplisert enn ved konvensjonell tilgangskontroll. Det skyldes at tilgangsbeslutningen kan være et utfall av ulike policyuttrykk, sammenholdt med en angitt kombinasjonsmetode. For visse typer kombinasjoner av policyer vil det kunne være vanskelig å avdekke entydig hvilken policy som egentlig er overtrådt.

Formelle policyspråk er primært utbredt i generell systemadministrasjon, og i mindre grad for å kontrollere tilganger til de enkelte dataelementer. Det er vanskelig å tenke seg at det ville reises avgjørende innvendinger mot policyer som autorisasjonsprinsipp. Argumentene ville i så fall sannsynligvis dreie seg mer om administrerbarhet enn om hvor godt policyer egner seg for å uttrykke tilgangskriterier.

9.5.2 Digital rettighetsforvaltning

Digital rettighetsforvaltning, som vanligvis omtales med sitt engelske akronym DRM (digital rights management) også på norsk, har sitt utspring i behovet for å kunne handle med og samtidig beskytte opphavsretten til digitale representasjoner av åndsverk. Et av flere formål med digital rettighetsforvaltning er å sikre at anskaffelse, bruk, videreformidling, salg og utlån av digitale verk ikke krenker noens rettigheter eller berettigede økonomiske interesser. En relativt omfattende kjerne i dette formålet har klare paralleller til kontroll med at tilgang til og videreformidling av opplysninger er berettiget. Digital rettighetsforvaltning skal i tillegg ivareta og balansere flere andre hensyn, som til dels favner videre enn bare å sikre at handlinger er berettigede.[794]

Den delen av digital rettighetsforvaltning som kan ha interesse som modell for å representere autorisasjon av tilgang til helseopplysninger er imidlertid den kjernen som dreier seg om hvordan digitale representasjoner vernes mot uberettigede handlinger. En sentral komponent, som finnes i en eller annen form i ulike DRM-systemer i markedet, er et formelt språk for å uttrykke digitale rettigheter, ofte omtalt som et REL.[795] Et slikt rettightsspråk kan beskrives som sammensatt av tre formål. Det ene er å representere informasjon om rettighetene til verket, det andre er å representere den adgang noen har ervervet til å bruke verket på en

[794] Mark Stefik (1997): «Shifting the possible: How trusted systems and digital property rights challenge us to rethink digital publishing». I: *Berkeley Technology Law Journal,* s. 137–159. Denne artikkelen reiser også andre spørsmål som har vist seg å by på langvarige problemer i dette feltet, som forholdet til bruk som er berettiget uten vederlag, og den skjøre balansen mellom konkurranse og samarbeid mellom aktørene i markedet.
[795] REL er en forkortelse for *Rights Expression Language*. Når *Digital* tilføyes foran, blir forkortelsen DREL.

bestemt måte, det tredje er å utøve, eller tvinge gjennom, en kontroll med at betingelsene overholdes.[796]

Den vanlige brukssituasjonen for slike rettighetsspråk er en form for handel, mellom autonome parter. Å avstå fra å erverve en tilgang til verket, eller å skaffe det i en annen form eller fra en annen forhandler i stedet, er ofte et gangbart alternativ for den om ikke er fornøyd med betingelsene. Dermed er det gode grunner til at DRM-tilnærmingen ikke lar seg overføre direkte til kontroll med helseopplysninger.[797] Helsepersonell står ikke fritt til å la være å bruke informasjonssystemet slik det er tilrettelagt fra virksomhetens side. Det er imidlertid likevel et par trekk ved digitale rettighetsspråk som bidrar til at det er interessant å ha med i en slik vurdering.

Et trekk, som i svært høy grad gir digital rettighetsinformasjon klebrighet på tvers av virksomhetsgrenser og ulike typer IT-systemer, er at representasjon av rettighetsinformasjonen gjerne er plassert i selve det digitale verket. En lisens til å bruke verket kan administreres på ulike vis, sentralt eller lokalt hos den enkelte databruker. En slik modell vil i prinsippet kunne gi en databruker, hvis han har «lisens» som omfatter for eksempel et konkret journalnotat eller en journaldel for en bestemt pasient, tilgang til dette uavhengig av hvilken virksomhet eller hvilket IT-system dataelementet befinner seg i. Databrukerens lisens kan endres eller trekkes tilbake. En tilbaketrekking vil fjerne tilgangen til det aktuelle dataelement, uansett hvor databrukeren prøver å få tak i det.

Et annet trekk er at digitale rettighetsspråk ofte opererer med mange forskjellige rettighetstyper. I tillegg til konvensjonelle rettighetstyper som å søke, lese, endre og slette, kan det også finnes egne rettighetstyper for å vise eller spille av, låne ut, selge, sende, kopiere, skrive ut, med mer.[798] De mange rettighetstypene henger sammen med at de ikke bare skal regulere betingelser for de ytterste databrukerne. Slike rettighetsspråk er laget for å forhandle og formidle rettigheter både til ulike ledd i en sammensatt forretningskjede, og til databrukeren som erverver lisensen ytterst i kjeden. Dermed vil rettigheter kunne uttrykkes på en slik måte at sentrale aktører i virksomhetene kan administrere rettigheter, både mellom virksomheter og

[796] Karen Coyle (2004): «Rights Expression Languages. A Report for the Library of Congress», s. 10.

[797] Det finnes flere teoretiske bidrag som drøfter bruk av en DRM-tilnærming for helseopplysninger, for eksempel Nicholas Paul Sheppard m. fl. (2009): «A Digital Rights Management Model for Healthcare» (konferanseartikkel) og Milan Petković m. fl. (2007): «Rights Management Technologies: A Good Choice for Securing Electronic Health Records?». I: *ISSE/SECURE 2007 Securing Electronic Business Processes*, s. 178–187. Begge disse artiklene stiller seg positive til mulighetene, men peker også på forskjeller som innebærer et behov for relativt omfattende tilpasninger før modellen egner seg for helseopplysninger.

[798] Det er imidlertid verdt å merke seg at selv om dette er et større spekter av rettighetstyper enn i konvensjonell tilgangskontroll, er det likevel ikke et rikere sett av modaliteter, slik som tilfellet er med formelle policyuttrykk. I rettighetsspråk for DRM-systemer kan man for eksempel ikke representere et «forbud» direkte. I likhet med det som gjelder i konvensjonell tilgangskontroll finnes forbud her bare som negasjon, eller fravær, av en tillatelse.

til den enkelte databruker, uten at den som administrer tilganger selv trenger å ha tilgang til å se dataelementenes innhold.

En side ved DRM-tilnærmingen som kan være betenkelig, når den anvendes på helseopplysninger, er at man ikke egentlig har kontroll med hvor hvert enkelt dataelement til syvende og sist blir av. Filer med digitale verk kan i utgangspunktet sendes hvor som helst, og befinne seg på en rekke forskjellige lagringsmedier. Ettersom filen er kryptert, vil ikke innholdet være tilgjengelig uten en gyldig lisens. Lisensen inneholder også den nøkkelen som trengs for å få tilgang til informasjonen, og å utføre de handlinger som lisensen omfatter. Rettighetshaver kan som regel leve godt med at slike filer kan finnes en rekke steder som han ikke engang vet om, så lenge bare den som har ervervet lisens kan få tilgang til innholdet. For helseopplysninger vil det derimot antakelig ikke være holdbart om en databehandlingsansvarlig virksomhet fullstendig frasier seg kontrollen over filene, selv om de er kryptert. Pasienten har et langvarig behov for at innholdet beskyttes, og det er vanskelig å avvise muligheten for at det som er en sterk kryptografisk beskyttelse i dag vil være utilstrekkelig et antall år frem i tiden.

Virksomhetens mulighet for å operasjonalisere egne beslutninger er i utgangspunktet god, men den er også til en viss grad tvetydig. Når dataelementene først er merket og kryptert, vil de kunne spres ut til samhandlende virksomheter og helsepersonell. Selve representasjonen av dataelementet lar seg vanskelig hente tilbake igjen, og det vil etter hvert kunne finnes i kryptert form som kopier hos ulike virksomheter og i ulike systemer. Den senere kontrollen man kan utøve over de dataelementene som blir spredt omkring består i å endre eller å trekke tilbake lisenser. Dersom en virksomhet velger å delegere lisenshåndteringen til de virksomhetene hvor dataelementet skal brukes, mister virksomheten kontroll med mottakende virksomhets konkrete håndhevelse av lisenspolitikken. Dersom avgivende virksomhet heller velger å håndtere lisensene selv kan de gjennomføre en enhetlig styring av tilgangene, men de vil ha mindre detaljkunnskap om databrukerens reelle tjenestelige behov enn det den mottakende virksomhet hvor databrukeren er ansatt har.

Ettersom tilgangstyringen til en viss grad er delegerbar, gir også dette autorisasjonsprinsippet relativt gode muligheter for å sikre at tilganger gis i samsvar med bestemmelser om taushetsplikt. Delegeringer kan begrenses og overstyres, noe som gir mulighet for en god balanse mellom operasjonaliserbarhet og avbildning.

En DRM-tilnærming gir svært lite rom for pasienters medinnflytelse. I prinsippet vil det bare være mulig å innfri en pasients eventuelle ønsker om å gi tilgang til flere personer. Begrensninger er vesentlig vanskeligere. Hvis man for eksempel skulle ønske å sperre et journaldokument, måtte man inndra alle lisenser som ga tilgang til dette dokumentet. Det

aktuelle dokumentet ville fremdeles finnes der det tidligere var spredt, men ingen ville lenger ha tilganger som gjør det mulig å se eller videreformidle innholdet. Om sperringen siden skulle oppheves, måtte det lages en ny, merket og kryptert versjon av journaldokumentet, med nye lisenser for de som igjen skulle ha tilgang.

Både felt A og felt B i overtredelsestaksonomien bør kunne holdes relativt små, fordi man har mulighet for å være temmelig presis i tildelingen av lisenser. Dataelementene kan i prinsippet «flyte fritt» rundt i ulike virksomheters informasjonssystemer, og være tilgjengelige for databrukere nærmest uavhengig av hvilket IT-system de bruker. Derfor trenger ikke et bestemt dataelements tilstedeværelse i et IT-system føre til at det blir utilsiktet og unødvendig tilgjengelig for en nærmest tilfeldig gruppe av databrukere som av andre årsaker har behov for vide tilganger i det aktuelle systemet. På den annen side kan det være vanskelig å avdekke overtredelser av type A, som altså vil si at databrukeren misbruker en faktisk tildelt lisens, fordi databrukeren kan velge å oppsøke forskjellige IT-systemer hver gang han ønsker å snoke i opplysninger. DRM-tilnærmingen kan bidra til at det blir mer krevende å skaffe full oversikt over hva den enkelte databruker gjør, og eventuelt å kartlegge tvilsomme handlingsmønstre.

DRM-systemer er utbredt innen sitt opprinnelige felt, som er kontroll med opphavsrettsbeskyttet digitalt materiale. Det har også vært foreslått brukt for helseopplysninger, men lite tyder på at det har fått særlig utbredelse i praksis. Enkelte av de kjente stridsspørsmålene som har omgitt DRM-systemer, som synspunkter på behov for å kunne overstyre kontrollsystemet når tilgang likevel er berettiget, eller debatten om innelåsing av verket i bestemte produkter på en måte som hemmer konkurranse og valgfrihet, er spesifikke for denne teknologiens opprinnelige anvendelsesområde, og ville neppe by på praktiske problemer dersom en DRM-tilnærming tas i bruk for helseopplysninger. Det kan derimot tenkes at modellen ville trenge en del tilpasninger for at den databehandlingsansvarlige skal kunne oppfylle sitt ansvar etter helseregisterloven.

9.5.3 Elektroniske agenter

Det siste prinsippet som presenteres og vurderes her er «elektroniske agenter», programvare som handler og forhandler på vegne av andre elektroniske eller menneskelige agenter.[799] Det

[799] Definisjoner av elektroniske agenter er et notorisk brysomt spørsmål. Dette utgangspunktet er basert på en ofte sitert artikkel som drøfter en rekke ulike definisjoner. En egnet definisjon for bruken av begrepet her lyder «agents are software entities that carry out some set of operations on behalf of a user», Stan Franklin og Art

er særlig denne «på vegne av»-egenskapen som vektlegges her. Derfor kan dette autorisasjonsprinsippet tenkes som et system av flere ulike agenter, som forhandler på vegne av ulike aktører om hvilke tilganger som skal gis i informasjonssystemet.

I likhet med digital rettighetsforvaltning er det handel og avtaleinngåelser mellom autonome aktører som er det praktiske feltet dette har oppstått i. Elektroniske agenter kan også sies å ha enkelte fellestrekk med en policybasert styringsstrategi, i den forstand at man er mer opptatt av å formulere uttrykk for hvilke tilstander man ønsker å oppnå i systemet enn å diktere en bestemt og entydig vei til målet. En annen definisjon peker på denne tilstandsorienterte siden ved elektroniske agenter:

> An *agent* is a system whose behavior is neither *accidental* nor strictly *causal*, but oriented to achieve a given state of the world. *Goal-governed* agents are able to achieve goals by themselves, by planning, executing, adapting and correcting actions.[800]

Elektroniske agenter er et litt omstendelig tema å bringe på bane som utgangspunkt for autorisasjoner, blant annet fordi det er omgitt av et vokabular som kan virke noe fremmedartet.[801] Teorien på dette området er rik på metaforer. En elektronisk agent kan ha mål, som er en representasjon av tilstandene den skal oppnå. Videre kan agenter ha en tro, som er antakelser om verden som den baserer vurderinger på, med mindre agenten får konkret informasjon som kan overstyre eller konkurrere med troen.[802] Det ser ikke ut til å være noen utpreget omfattende litteratur som anbefaler eller vurderer bruk av elektroniske agenter til å styre tilgang til helseopplysninger, men enkelte eksempler finnes.[803]

Det en elektronisk agent «gjør», ut fra disse definisjonene, er å være et program som kjøres, regelmessig eller helst kontinuerlig, i et IT-system. Det har fått noen definerte representasjoner av fullmakter og målsituasjoner gjennom et (riktig gjettet!) agentkommunikasjonsspråk. For å nå sitt tildelte mål, kan agenten undersøke alternativer, prøve å forutsi

---

Graesser (1997): «Is It an Agent, or Just a Program? A Taxonomy for Autonomous Agents». I: *Intelligent Agents III. Agent Theories, Architectures, and Languages*, s. 21–35.

[800] Rosaria Conte m. fl. (1999): «Autonomous Norm Acceptance». I: *Intelligent Agents V: Agent Theories, Architectures, and Languages (5th International Workshop, ATAL'98, Paris, France, July 1998. Proceedings)*, s. 99–112. (s. 103, original utheving).

[801] Christen Krogh og Henning Herrestad (1999): «Hohfeld in cyberspace and other applications of normative reasoning in agent technology». I: *Artificial Intelligence and Law,* s. 81–96.

[802] «Tro» er her en oversettelse av flertallsordet «beliefs». Vokabularet har sitt utgangspunkt i at svært mange systemer best forstås ut fra en betraktning om intensjonalitet, og ikke ut fra betraktninger om fysiske lover eller designede egenskaper. Jf. Daniel C. Dennett (1998): *The intentional stance*, som argumenterer for at denne synsvinkelen egentlig er godt innarbeidet, vi bruker den om alt fra en enkel termostat til biologisk evolusjon.

[803] For eksempel Maged N. Kamel Boulos m. fl. (2006): «Using software agents to preserve individual health data confidentiality in micro-scale geographical analyses». I: *Journal of Biomedical Informatics,* s. 160–170.

mulige utfall, kommunisere med andre agenter om alternativer og utfall, reagere på endringer i sine digitale omgivelser, og eventuelt beslutte noe eller utløse hendelser.[804]

Beskrivelsen så langt er kanskje i overkant abstrakt, et tenkt eksempel bidrar muligens til å konkretisere hva dette kan innebære for kontroll med helseopplysninger: Et sykehus har en elektronisk agent, med et uttrykt mål som går ut på at alt helsepersonell som samarbeider om behandlingen av en pasient skal ha tilgang til dennes journal.[805] Agenten har en tro, som går ut på at pasienter ikke vil motsette seg dette. Pasient Peder Ås har sin egen agent, som har som mål at den nysgjerrige svigerinnen Marte Kirkerud ikke skal få se opplysninger om ham. Dette vil overstyre agentens tro, i de situasjoner hvor den hadde vært tilbøyelig til å gi Marte Kirkerud tilgang. Når Marte-filteret slår inn for åttende gang, vil kanskje sykehusets agent også selv ha lært hva Peder Ås mener om dette. En annen pasient, Lars Holm, har en egen agent som motsetter seg alt som motsettes kan, med mindre han selv gir klarsignal. På den måten forblir dette en innsigelsesrett for Peder Ås, mens Lars Holm har brukt sin agent til i realiteten å konvertere denne bestemmelsen i helsepersonelloven fra innsigelsesrett til et krav om eksplisitt samtykke. Det er dette målet, «jeg vil gi uttrykkelig samtykke i alle de tilfeller hvor det kan gis anledning til det», Lars Holm har instruert sin agent om å forfølge.

Eksemplet kan trekkes litt videre, man kan anta at agenten i utgangspunktet ikke har noen tro som forutser om det er nødvendig eller ikke nødvendig at samarbeidende helsepersonell får disse opplysningene. Det må helsepersonellet som har taushetsplikten angi konkret. Kanskje tillater sykehuset at agenten lærer seg når deling av opplysninger er nødvendig? Læringen kan for eksempel se slik ut: Når en bestemt behandlingsprosedyre er utført femti ganger, og det har vært angitt at det var nødvendig å gi opplysninger videre til samarbeidende personell i minst nitti prosent av tilfellene, får agenten for ettertiden lov til å tro at opplysninger skal gis videre, helt til den eventuelt får motsatt beskjed. Denne troen bør kanskje avlæres dersom manuell overstyring blir hyppig, for eksempel hvis andelen situasjoner der opplysninger skal gis til samarbeidende personell synker til under åtti prosent. Alle de tre agentene i eksemplet har fått sine mål, fullmakter og initielle antakelser om verden definert på forhånd. I prinsippet kan de også finne og lære seg egne veier til det målet som er definert, innen de fullmakter de har fått tildelt.

Det har vært stilt en rekke både rettslige og rettsteoretiske spørsmål om elektroniske agenter, som vil kunne ha betydning for vurderingen av hvor godt egnet dette kan være som

[804] Disse egenskapene, eller ferdighetene, vil i prinsippet være felles for elektroniske og humane agenter. Jf. Vivien Burr (2003): *Social constructionism*, s. 194: «We can imagine what would happen if we were to act in a certain way and can therefore consider alternative actions, which is a way of describing agency.»
[805] Eksemplet er basert på en lek med unntak fra taushetsplikt etter helsepersonelloven § 25(1).

autorisasjonsprinsipp for tilgang til helseopplysninger. Et av disse spørsmålene gjelder hvilken status en elektronisk agent vil ha etter personopplysningsretten.[806] Et annet og mer teoretisk spørsmål er hvorvidt en elektronisk agents handlingsnormer, som er uttrykt i et formelt språk og som gjelder på vegne av prinsipalen, er prosessuelle eller materielle.[807] Man kan også støte på intrikate spørsmål om maktskjevhet, målkonflikter og agenter som velger andre handlinger enn de burde ha valgt.[808] En fullstendig drøfting av elektroniske agenters egnethet som autorisasjonsprinsipp måtte ha tatt disse spørsmålene, antakelig også mange flere, med i betraktningen. Det som følger her er ingen komplett redegjørelse for alle slike spørsmål, vurderingen er begrenset til en representasjonsmessig egnethet, ut fra de samme vurderingskriteriene som er brukt for de foregående autorisasjonsprinsippene.

Alle de tre første vurderingskriteriene, operasjonalisering av virksomhetens beslutninger, samsvar med bestemmelser om taushetsplikt, og pasienters medinnflytelse, kan i utgangspunktet ivaretas godt gjennom et system av autonome agenter. Dersom man velger, som i det lille eksemplet ovenfor, at bare sykehuset og pasientene får bli representert av agenter, vil operasjonalisering og medinnflytelse komme godt ut. En styrking av mulighetene for å avbilde bestemmelser om taushetsplikt kan kanskje ivaretas gjennom at helsepersonell også har sine agenter. Det kan imidlertid hefte noe mer tvil ved hvor mye man vinner ved å la helsepersonell ha egne agenter i systemet: For det første er det grenser, som muligens kan være noe uklare, for hvor autonome helsepersonell egentlig er vis à vis virksomheten. For det andre vil det kunne gå ut over pasienten dersom enkelte helsepersonell inntar en passiv holdning til sin agent, samtidig som systemet forutsetter at alle tar aktivt stilling til hva egen agent skal oppnå.

En toparts forhandling mellom virksomhetens og pasientens agenter er antakelig mest ryddig og oversiktlig. Det kan imidlertid fremdeles gjenstå et problem med de pasientene som ikke ønsker å engasjere seg, og derfor lar være å utstyre sin agent med mål og antakelser for å øve medinnflytelse. Dette er i grunnen det samme problemet som man har i autorisasjonsprinsippet *pasientstyrt tilgangskontroll*, faren for passive pasienter må håndteres ved at

[806] Dette er et spørsmål som har flere sider, blant annet hvorvidt agenter i seg selv *er* personopplysninger, om en agent kan gi gyldig samtykke på vegne av prinsipalen, og om kravet til å informere den registrerte kan være tilstrekkelig ivaretatt ved å informere agenten. Disse spørsmålene, med flere, er drøftet i Lee A. Bygrave (2001): «Electronic Agents and Privacy: A Cyberspace Odyssey 2001». I: *International Journal of Law and Information Technology,* s. 275–294.

[807] Guido Boella og Leendert van der Torre (2008): «Substantive and procedural norms in normative multiagent systems». I: *Journal of Applied Logic,* s. 152–171.

[808] Alexander Artikis m. fl. (2009): «Specifying Norm-Governed Computational Societies». I: *ACM Transactions on Computational Logic (TOCL),* s. 1–42.

virksomheten sørger for et robust minstenivå i vernet av helseopplysninger uavhengig av om pasienten vil øve medinnflytelse eller ikke.

Agentenes mål og fullmakter trenger i utgangspunktet ikke begrenses av virksomhetsgrenser eller IT-systemer. Likevel er man avhengig av en betydelig samordning for å sikre at det som agentene lykkes i å forhandle seg frem til faktisk blir respektert, og iverksatt på en konsekvent måte, hos ulike samarbeidende virksomheter.

Etterprøvbarheten, for å avdekke overtredelser, vil antakelig være svak. Dersom en databruker ønsker tilgang, er det i prinsippet pasienten selv som gir tilgangen via sin elektroniske agent. Virksomheten kan kanskje se etter mønstre av overdreven eller uventet aktivitet blant sine databrukere, men det vil være enda vanskeligere enn ellers for virksomheten å slutte direkte fra hva databrukeren gjør til en tvil om hvorvidt det han gjør er berettiget.

Som det meste annet som gjelder elektroniske agenter, er også utbredelsen noe som det kan være litt vanskelig å uttale seg generelt om. Det skyldes at idégrunnlaget ofte fremstilles, som her, idealtypisk og med markante og noe fremmedartede metaforer. I praktisk utbredelse, som for eksempel i selvbetjente bookingsystemer og lignende, vil innslaget av målorienterte elektroniske agenter ofte fremstå som mer jordnært og nøkternt. Dersom man ser for seg en kombinasjon av flere autorisasjonsprinsipper, kanskje særlig de tre variantene *tilgang basert på behandlingsopplegg*, *pasientstyrte tilganger* og *rollebasert tilgang*, kunne en slik kombinasjon i praksis begynne å ligne en moderat versjon av et system for autonome agenter.

	Generelle og utbredte autorisasjonsprinsipper				Aktualiseringsmekanismer		
	Direkte tilgang og sentralisert kontroll	Indirekte tilgang og sentralisert kontroll (roller)	Direkte og delegerbare tilganger	Indirekte og delegerbare tilganger	Merking av aktive pasient-relasjoner	Nødretts-tilganger	
Operasjonalisering av virksomhetens kriterier	+	+ +	–	+	+	+	
Avbilde bestemmelser om taushetsplikt	+	–	+	+	–	+	
Pasienters medinnflytelse	+	–	+	– –	–	–	
Etterprøvbarhet	–	–	+	+	+	+	
Teknologiens utbredelse og anseelse	– –	+ +	–	–	+	+	

9.6 Sammenligning av prinsipper

Av de autorisasjonsprinsippene som har vært presentert og vurdert er det ingen som kan sies å komme helskinnet gjennom alle vurderingskriteriene. Vurderingene av hvert prinsipp viser kanskje først og fremst at det er mange nyanser som gjør det vanskelig å gjennomføre direkte sammenligninger. Som en sterk forenkling, kanskje også overforenkling, kan man likevel ta sjansen på å oversette vurderingene ovenfor til et slags poengsystem, der hvert autorisasjonsprinsipp tildeles ett eller to plusstegn eller minustegn for hvert vurderingskriterium.

Autorisasjonsprinsippene er gjennomgående vurdert hver for seg, men som antydet under enkelte av vurderingene kunne man også se for seg mellomløsninger eller kombinasjoner av autorisasjonsprinsipper.

Sammenligningen av «poengsummer» viser bortimot likt utfall for flere av prinsippene. Skulle man utpeke en slags vinner basert på tabellens skjematiske oppstilling, ville det være nærliggende å peke på autorisasjonsprinsippet *beslutningsstyrt tilgangskontroll*, fordi det både skårer jevnt høyt generelt, og fordi det kommer best ut av kriteriet samsvar med bestemmelser om taushetsplikt spesielt. Med store forbehold kunne man si at dette autorisasjonsprinsippet blir det direkte svaret på avhandlingens problemstilling. Det samlede arbeidet med disse spørsmålene peker imidlertid heller i retning av at det er de mange komplekse sammenhengene, og fraværet av et entydig svar, som er vurderingenes egentlige resultat.

	Forløpsbasert autorisasjon		Medinnflytelsesbasert autorisasjon		Alternativer til konvensjonell autorisasjon		
	Beslutningsstyrt tilgangskontroll	Tilganger basert på behandlings-opplegg	Pasientstyrt tilgangskontroll	Pasientholdte data	Spesifikasjons-språk for tilgangspolitikk	Digital rettighets-forvaltning	Elektroniske agenter
	+	+ +	–	–	+ +	+	+ +
	+ +	+	+	–	+	+	+
	–	–	+ +	+ +	–	– –	+ +
	++	+	–	+	–	–	–
	–	–	–	+	+ +	+	–

10 Avslutning

Avhandlingens emne er tilgang til og videreformidling av helseopplysninger. Hovedperspektivet er kontroll med tilgang og videreformidling som normalt vil være berettiget, altså handlinger som i de aller fleste tilfeller skal eller bør finne sted. Det sentrale forskningsspørsmålet er «hva slags teknologiske representasjoner av regler om tilgang til og videreformidling av helseopplysninger er best egnet til å innfri kravet til samsvar?» Spørsmålet er motivert av helseregisterlovens føringer på området, først og fremst dette tosidige kravet: «Tilgang kan bare gis i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt».[809] Denne avhandlingen er et forsøk på å besvare spørsmålet gjennom en tverrfaglig analyse, mer preget av et ønske om å fange inn problemets bredde enn av å gå dypest mulig inn i detaljene. Analysen har hatt fire innfallsvinkler: Aktørene, reguleringen, praksisen og teknologien. Hver av disse rommer i seg selv atskillig flere aspekter og mer dynamikk enn det som drøftes i avhandlingen. Hovedvekten er lagt på sammenhenger mellom innfallsvinklene, og hvilken betydning disse sammenhengene har for problemstillingen.

Aktørperspektivet finner man antydet ved at tilganger gis. De gis av noen, og til noen. Databehandlingsansvarlige, som i hovedsak er virksomheter, kan tildele tilganger til fysiske databrukere, som i hovedsak er helsepersonell. Det er et komplisert samspill mellom helsepersonells faglige autonomi og virksomheters «sørge for»-ansvar, virksomheters og helsepersonells relasjoner til pasientene, og virksomheters og helsepersonells relasjoner til overordnede myndigheter. Forholdet mellom helsepersonell og virksomheter er i bevegelse. Det er flere trekk som peker i retning av at behandling av helseopplysninger i økende grad blir virksomhetens anliggende, og i tilsvarende mindre grad handler om helsepersonellets internaliserte profesjonsnormer.

Reguleringen av tilgang til og videreformidling av helseopplysninger har to hovedkomponenter. Den ene er komponenten er generelle krav til tilgangskontroll, som en del av informa-

[809] Helseregisterloven § 13(1) annet punktum.

sjonssikkerhetsarbeidet. Den andre komponenten er konkrete regler om når det kan gjøres unntak fra taushetsplikten, og på hvilke betingelser. Kravene til informasjonssikkerhet er forankret i personopplysningsretten, og basert på internkontroll som reguleringsmetode. Det er en form for prosessregler som er svært fleksible, og gir virksomhetene stort handlingsrom. Et lite paradoks blir likevel påpekt, i det at virksomhetenes store handlingsrom bare har gyldighet innenfor virksomhetens grenser. Internkontrollbasert informasjonssikkerhet gir lite støtte for tiltak som ivaretar sikkerheten når helseopplysninger formidles til aktører utenfor virksomheten. Det finnes også en konkret, lovbestemt begrensning i den adgangen en virksomhet har til å tildele tilgang til personer som ikke er underlagt virksomhetens instruksjonsmyndighet.[810]

Taushetsplikten, som primært er regulert i helsepersonelloven, er i utgangspunktet individuell. Den binder hver enkelt som behandler helseopplysninger. Unntakene er regulert uttømmende, selv om det ligger noe fleksibilitet i at det i mange tilfeller må utøves et faglig skjønn ved vurdering av om den situasjonen som unntaksbestemmelsen gjelder faktisk har inntruffet. Den profesjonsbestemte taushetsplikten er imidlertid ikke rammet inn av virksomhetsgrenser, på det området er den helserettslige reguleringen mest fleksibel.

Grunnleggende sett er de to hovedkomponentene forbundet med ulike aktørgrupper. Informasjonssikkerheten er virksomhetens ansvar, mens taushetsplikten er profesjonsutøvernes ansvar. I avhandlingen er det lagt stor vekt på å tydeliggjøre forskjellene mellom disse to hovedkomponentene i reguleringen, selv om det også trekkes frem enkelte forhold som minsker avstanden mellom dem. Et av forholdene som minsker avstanden mellom disse to hovedkomponentene er at det er en del av virksomhetenes «sørge for»-ansvar å tilrettelegge for at taushetsplikten blir overholdt. Et annet forhold er at det både innen personopplysingsretten og helseretten finnes begrensede, men viktige, rettigheter til kontroll og medvirkning for pasienten. Likevel er det avstanden mellom disse to hovedkomponentene som er mest slående. Helseregisterlovens tilsynelatende enkle bestemmelse om når tilgang kan gis, omfatter både tilgangskontroll som del av informasjonssikkerhetsarbeidet og taushetsplikten som en del av grunnlaget for å berettige tilgang. Kriteriet «i den grad dette er nødvendig for vedkommendes arbeid» følger en informasjonssikkerhetsfaglig logikk, mens «i samsvar med gjeldende bestemmelser om taushetsplikt» peker på de helserettslige profesjonspliktene.

Analysen av praksis består til dels av en redegjørelse for hva helseopplysninger er, hvordan de dokumenteres og organiseres, og ulike typer systemer der de behandles. Praksisen er i stor

[810] Helseregisterloven § 13(1) første punktum. Etter lovendring 19. juni 2009 nr. 68 er det adgang til å fravike denne begrensningen ved forskrift, jf. § 13(2).

grad influert av både rettslig regulering og av ulike aktørgruppers agendaer og perspektiver. Grunnen til at denne siden ved praksis er viktig i dette arbeidet, er at organiseringen av opplysninger og informasjonssystemer, og opplysningenes kvalitet, har direkte betydning for de måtene man kan representere tilgangskriterier på.

En annen side ved praksis, som har fått noe mindre plass i avhandlingen, er empirisk materiale om helsepersonells og virksomheters erfaring med og etterlevelse av regler om håndtering av helseopplysninger. Empirien viser at regelbrudd forekommer. I tillegg gir de empiriske dataene noen holdepunkter for å vurdere realismen i opplegg for selvautorisering under ansvar. Viljen til, og mulighetene for, å avdekke og reagere på regelbrudd vil også ha en viss betydning for hvilke teknologiske valg som er best egnet.

Den teknologiske innfallsvinkelen i avhandlingen er en drøfting av autorisasjonsprinsipper, og hvordan reguleringen kan representeres i tilgangskontrollmekanismer. Beskrivelsene av representasjonsmåter er lagt på et relativt generelt nivå, og ikke knyttet til konkrete produkter eller implementasjoner. Alle de vurderte autorisasjonsprinsippene finnes som idégrunnlag i eksisterende eller foreslåtte tilgangskontrollmekanismer. Autorisasjonsprinsippene er vurdert og sammenlignet ut fra kriterier som er utarbeidet gjennom avhandlingens innledende deler. Hvert av prinsippene har sterke og svake sider, ingen av dem peker seg ut som overlegent bedre enn de andre.

Problemstillingen inneholder et spørsmål om hvilken representasjonsmåte som er best egnet. Dersom man tolker dette spørsmålet helt snevert, i retning av at best egnet betyr det autorisasjonsprinsippet som fører til en mest mulig riktig representasjon etter lovens bokstav, faller den samlede vurderingen, etter gjeldende regulering, ned på *beslutningsstyrt tilgangskontroll*. De innvendingene som kan reises, særlig de som gjelder høye krav til datakvalitet og faren for kunstig produksjon av beslutningspunkter, er det imidlertid all grunn til å ta alvorlig.

En litt romsligere forståelse av hva som kan være best egnet tilsier kanskje at de autorisasjonsprinsippene som gir mer kontroll til pasienten bør ha et fortrinn, selv om gjeldende regulering ikke tilkjenner pasientmedvirkning stort mer enn moralsk støtte og enkelte punktvise, betingede rettigheter. Det kunne være fristende å gi sin støtte til elektroniske agenter som autorisasjonsprinsipp, for å integrere ulike aktørgruppers normer, interesser og posisjoner i et felles rammeverk for å håndtere tilgang og videreformidling. Det innebærer imidlertid et større sprang både teknologisk og kognitivt enn de øvrige prinsippene. Selv med teknologien på plass ville det være vanskelig å få overblikk over hva et autorisasjonsprinsipp basert på autonome, elektroniske agenter krever av aktørene, av organiseringen av helseopplysningene, og av datakvaliteten.

Det er verdt å merke seg at hele feltet, både reguleringen, teknologien og aktørgruppenes forventninger, er i bevegelse. Samtidig er helseopplysninger et stort felt. Det er kontrollen med de store volumene av helseopplysninger som til syvende og sist er viktig, lite er vunnet om man bare lykkes innenfor enkelte, spredte informasjonssystemer. Spørsmålet om hva som skal regnes som best egnet bør derfor antakelig også omfatte mer trauste elementer som at autorisasjonsprinsippene er enkle, kan iverksettes med kjent og robust teknologi, og at de bør stille moderate krav til hvilke opplysninger om den aktuelle helsehjelpen eller pasienten som må være på plass for å avgjøre et spørsmål om tilgang.

Litteraturliste

A: Artikler, bøker, rapporter og diverse

A Declaration on the Promotion of Patients' Rights in Europe (1994), World Health Organization, Regional Office for Europe. (Amsterdamerklæringen).

Aksnes, Bjarte, og Magnus Alsaker (2005): «Elektronisk tilgang til helseopplysninger – utfordringer og mulige tiltak». Høykom-rapport nr. 506. Oslo, Norges forskningsråd.

Akutt- og utredningstilbudet for ungdom på åpne institusjoner i Oslo. (2009). 2. juni 2009. (Brev fra fire barnevernsansatte til Bystyrets helse- og sosialkontor).

Alexy, Robert (2002): *A Theory of Constitutional Rights*. Oxford: Oxford University Press.

Andenæs, Kristian (1989): «The law and the nonlegal professionals: on decision-making by medical doctors and social workers». I: *International journal of law and psychiatry*. Årg. 12, nr. 4, s. 12.

——— (2006): «Om maktens rettsliggjøring og rettsliggjøringens maktpotensial». I: *Tidsskrift for samfunnsforskning*. Årg. 47, nr. 4, s. 587–599.

Andresen, Herbjørn (1999): «Om samsvaret mellom et IT-system og et rettslig regelverk, systemdokumentasjon som viser til rettskilder». Hovedfagsoppgave, Universitet i Oslo, Avdeling for forvaltningsinformatikk.

——— (2008a): «Systemintegrasjon i e-forvaltningen og følgene for dokumentasjon av systemenes rettslige innhold». I: Jansen, Arild og Dag Wiese Schartum (red.): *Elektronisk forvaltning på norsk: Statlig og kommunal bruk av IKT*. Bergen: Fagbokforlaget. s. 227–243.

——— (2008b): «Kven skal trøyste Hypomone? Eit kammerspel i tre akter om vern av pasientopplysningar » [Drama/fiksjon]. I: *Syn og Segn*. Årg. 114, nr. 1, s. 52–61.

——— (2008c): «The Attitude of Norwegian Healthcare Professionals Towards eHealth». I: *The Journal on Information Technology in Healthcare*. Årg. 6, nr. 6, s. 429–440.

——— (2009): «The Policy Debate on Pseudonymous Health Registers in Norway». I: Fred, Ana, Joaquim Filipe og Hugo Gamboa (red.): *Biomedical Engineering Systems and Technologies*. Berlin Heidelberg: Springer. s. 413–424.

——— (2010): «Tilgang til og videreformidling av helseopplysninger. Regulering og kontroll på tvers av IT-systemer og organisatoriske grenser». Manuskript innlevert til bedømmelse for Ph.d-graden. Avdeling for forvaltningsinformatikk, Juridisk fakultet, Universitetet i Oslo.

Andresen, Herbjørn, og Olaf Gjerløw Aasland (2008): «Helsepersonells håndtering av pasientopplysninger» [Originalartikkel]. I: *Tidsskrift for Den norske legeforening*. Årg. 128, nr. 24, s. 2823–2827.

Apitzsch, Felix, Stefan Liske, Thomas Scheffler, og Bettina Schnor (2008): «Specifying Security Policies For Electronic Health Records». (Konferanseartikkel presentert på Healthinf 2008) Funchal, Madeira, Portugal.

Artikis, Alexander, Marek Sergot, og Jeremy Pitt (2009): «Specifying Norm-Governed Computational Societies». I: *ACM Transactions on Computational Logic (TOCL)*. Årg. 10, nr. 1, s. 1–42.

Ashley, Kevin D. (1991): *Modeling Legal Arguments: Reasoning with Cases and Hypotheticals*. London: MIT Press.

Austin, John Langshaw (1962): *How to do things with words*. Cambridge, Massachusetts: Harvard University Press.

Ayres, Ian, og John Braithwaite (1992): *Responsive Regulation: Transcending the Deregulation Debate*. New York: Oxford University Press.

Backer, Inge Lorange (2002): «Miljöskydd och ekonomiskt utnyttjande – principen om hållbar utveckling». *Förhandlingarna vid det 36. nordiska juristmötet i Helsingfors 15.-17. augusti 2002*. Jyväskylä: Kirjapaino. s. 113–141.

Becker, Moritz Y. (2007): «Information governance in NHS's NPfIT: A case for policy specification». I: *International Journal of Medical Informatics*. Årg. 76, nr. 5-6, s. 432–437.

Bell, D. Elliot, og Leonard J. LaPadula (1973): «Secure Computer Systems: Mathematical Foundations». I: *MITRE Technical Report 2547 vol. I*.

Bench-Capon, Trevor, og Marek Sergot (1988): «Towards a rule-based representation of open texture in law». I: *Computer power and legal language*. s. 39–61.

Berg, Jens Petter (1999): «Personopplysningsvern i et nytt årtusen – kritikk av personopplysningslovproposisjonen». I: *Kritisk Juss*. Årg. 26, nr. 4, s. 351–377.

Berg, Marc, og Geoffrey Bowker (1997): «The Multiple Bodies of the Medical Record: Towards a Sociology of an Artifact». I: *The Sociological Quarterly*. Årg. 38, nr. 3, s. 513–537.

Beyleveld, Deryck, og Roger Brownsword (2007): *Consent in the law*. Oxford: Hart Publishing.

Bing, Jon (1977): «Automatiseringsvennlig lovgivning». I: *Tidsskrift for Rettsvitenskap*. Årg. 90, s. 195–229.

——— (1983): *EDB: mulighet og problem ved forenkling av regelverk*. Oslo: Universitetsforlaget.

——— (1998): *Landskap med tegn: en liten bok om informasjonsteknologi og informasjonspolitikk*. Oslo: Pax.

——— (2008): «Notions of sensitive personal data». I: Verónica, Marie og Pablo Palazzi (red.): *Défis du droit à la protection à la vie privée/Challenges of Privacy and Data Protection Law*. Bruxelles: Centre de Documentation C.R.I.D, Facultés universitaires Notre-Dame del la Paix de Namur. s. 191–208.

Black, Julia (2000): «Proceduralizing Regulation: Part I». I: *Oxford Journal of Legal Studies*. Årg. 20, nr. 4, s. 597–614.

Blix, Bodil Hansen (2005): ««Korthuset». Sykepleieres erfaringer med elektronisk sykepleiedokumentasjon i egen praksis» Mastergradsoppgave. Avdeling for sykepleie og helsefag, Universitetet i Tromsø.

Boella, Guido, og Leendert van der Torre (2008): «Substantive and procedural norms in normative multiagent systems». I: *Journal of Applied Logic*. Årg. 6, nr. 2, s. 152–171.

Boulos, Maged N. Kamel, Qiang Cai, Julian A. Padget, og Gerard Rushton (2006): «Using software agents to preserve individual health data confidentiality in micro-scale geographical analyses». I: *Journal of Biomedical Informatics*. Årg. 39, nr. 2, s. 160–170.

Braithwaite, John (1982): «Enforced Self-Regulation: A New Strategy for Corporate Crime Control». I: *Michigan Law Review*. Årg. 80, s. 1466–1507.

Brownsword, Roger (2005): «Code, control, and choice: why East is East and West is West». I: *Legal Studies*. Årg. 25, nr. 1, s. 1–21.

Burr, Vivien (2003): *Social constructionism*. 2 utgave. London: Routledge.

Bygrave, Lee A. (1996): «Ensuring right information on the right person(s): legal controls of the quality of personal information, Part 1». Forvaltningsinformatisk notatserie 4/96, Universitetet i Oslo, Avdeling for forvaltningsinformatikk.

——— (2001): «Electronic Agents and Privacy: A Cyberspace Odyssey 2001». I: *International Journal of Law and Information Technology*. Årg. 9, nr. 3, s. 275–294.

——— (2002): *Data protection law: approaching its rationale, logic and limits*. Dortrecht: Kluwer.

Campbell, Roy, Jalal Al-Muhtadi, Prasad Naldurg, Geetanjali Sampemane, og M. Dennis Mickunas (2003): «Towards Security and Privacy for Pervasive Computing». I: Okada, Mitsuhiro, Benjamin Pierce, Andre Scedrov, Hideyuki Tokuda og Akinori Yonezawa (red.): *Software Security — Theories and Systems*: Springer. s. 77–82.

Cate, Fred H. (2006): «The failure of fair information practice principles». I: Winn, Jane K. (red.): *Consumer Protection in the Age of the Information Economy*. Aldershot: Ashgate. s. 341–377.

Chadwick, Ruth F. (1997): «The philosophy of the right to know and the right not to know». I: Chadwick, Ruth F., Mairi Levitt og Darren Shickle (red.): *The Right to know and the right not to know*. Aldershot: Ashgate. s. 13–22.

Clark, David D., og David R. Wilson (1987): «A Comparison of Commersial and Military Computer Security Policies». (Konferanseartikkel presentert på IEEE Symposium on Security and Privacy).

Conte, Rosaria, Cristiano Castelfranchi, og Frank Dignum (1999): «Autonomous Norm Acceptance». I: Müller, Jörg P., Munindar P. Singh og Anand S. Rao (red.): *Intelligent Agents V: Agent Theories, Architectures, and Languages (5th International Workshop, ATAL'98, Paris, France, July 1998. Proceedings)*. Berlin Heidelberg: Springer-Verlag. s. 99–112.

Corrigan, Oonagh (2003): «Empty ethics: the problem with informed consent». I: *Sociology of Health & Illness*. Årg. 25, nr. 7, s. 768–792.

Coyle, Karen (2004): «Rights Expression Languages. A Report for the Library of Congress».

Daconta, Michael C., Leo J. Obrst, og Kevin T. Smith (2003): *The Semantic Web: a guide to the future of XML, Web services, and knowledge management*. Indianapolis: Wiley.

Damianou, Nicodemos, Naranker Dulay, Emil Lupu, og Morris Sloman (2001): «The ponder policy specification language». (Konferanseartikkel presentert på Workshop on Policies for Distributed Systems and Networks) Bristol, UK.

Datatilsynet: «Om Datatilsynet – Datatilsynets oppgaver» *http://www.datatilsynet.no/templates/Page____954.aspx* [Lesedato: 14.04.2010].

Davidson, Donald (1996): «The Folly of Trying to Define Truth». I: *The Journal of Philosophy*. Årg. 93, nr. 6, s. 263–278.

Dennett, Daniel C. (1998): *The intentional stance*. Cambridte, Mass: MIT press.

Din patientjournal: Enkätundersökning (2005). Uppdragsgivare: Patientdatautredningen. Stockholm, Statistiska Centralbyrån.

Djønne, Eirik, Tove Grønn, og Tor Hafli (1987): *Personregisterloven med kommentarer*. Oslo: TANO.

Douglas, Mary (1992): *Risk and Blame: Essays in Cultural Theory*. London: Routledge.

Easterbrook, Frank H. (1996): «Cyberspace and the Law of the Horse». I: *University of Chicago Legal Forum*. Årg. 1996, s. 207–216.

Eckhoff, Torstein, og Nils Kristian Sundby (1991): *Rettssystemer: systemteoretisk innføring i rettsfilosofien*. 2. utgave. Oslo: Tano. [1. utgave 1976].

Eggen, Kyrre (2004): «Ansattes ytringsfrihet. Rettslige bånd eller gyldne lenker?». I: *Arbeidsrett*. Årg. 1, nr. 1, s. 2–23.

Ekeland, Tor-Johan (2004): «Autonomi og evidensbasert praksis». Arbeidsnotat 6/2004, Senter for profesjonsstudier, Høgskolen i Oslo.

Elgesem, Dag (1999): «The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data». I: *Ethics and Information Technology*. Årg. 1, nr. 4, s. 283–293.

Ellingsen, Gunnar, og Eric Monteiro (2003): «Mechanisms for producing a working knowledge: Enacting, orchestrating and organizing». I: *Information and Organization*. Årg. 13, nr. 3, s. 203–229.

Eng, Svein (2007): *Rettsfilosofi*. Oslo: Universitetsforlaget.

EPJ Monitor. Årsrapport 2008. Oversikt over utbredelse og bruk av IKT i helsetjenesten (2008), Helsedirektoratet.

Europarådets konvensjon og rekommandasjoner om persondatabeskyttelse (1981). Europarådets konvensjon 28 januar 1981 nr. 108.

Ferraiolo, David F., og D. Richard Kuhn (1992): «Role-Based Access Control». (Konferanseartikkel presentert på 15th NIST-NCSC National Computer Security Conference) Gaithersburg, MD.

Forslag til regler om arbeidsgivers tilgang til Ansattes e-post mv. – endring av personopplysningsloven § 3 og § 46, nytt kapittel i personopplysningsforskriften og ny bestemmelse i arbeidsmiljøloven (2006), Fornyings- og administrasjonsdepartementet. (Høringsnotat, 17. oktober 2006).

Franklin, Stan, og Art Graesser (1997): «Is It an Agent, or Just a Program? A Taxonomy for Autonomous Agents». I: Müller, Jörg P., Michael J. Wooldridge og Nicholas R. Jennings (red.): *Intelligent Agents III. Agent Theories, Architectures, and Languages*: Springer Berlin Heidelberg. s. 21–35.

Frich, Jan C., og Per Fugelli (2005): «Bør pasienten kunne skrive i egen journal?» [Debattartikkel]. I: *Tidsskrift for Den norske lægeforening*. Årg. 125, nr. 7, s. 918.

Færden, Anders (1897): «Lægers taushedspligt». I: *Tidsskrift for Den norske lægeforening*. Årg. 17, nr. 8, s. 171–187.

Førde, Reidun, og Åsmund Hodne (2004): «Rådet for legeetikk 1985 - 2001». I: *Tidsskrift for Den norske lægeforening*. Årg. 124, nr. 7, s. 936–938.

Giddens, Anthony (1984): *The constitution of society: outline of the theory of structuration*. Cambridge: Polity Press.

Gode helseregistre – bedre helse (2009), Helse- og omsorgsdepartementet. (Strategi for modernisering og samordning av sentrale helseregistre og medisinske kvalitetsregistre 2010-2020).

Goffman, Erving (1961): *Asylums. Essays on the social situation of mental patients and other inmates*. New York: Doubleday.

Graver, Hans Petter (1984a): «Fleksibilitet som reguleringsteknikk - mot en anarkistisk rettsform». I: *Retfærd. Nordisk Juridisk Tidsskrift*. Årg. 26, s. 59–68.

——— (1984b): «Sikkerhetsaspekter ved utkastet til ny petroleumslov med forskrifter». I: *Lov og Rett*. Årg. 23, s. 140–153.

——— (2004): «Bevisbyrde og beviskrav i forvaltningsretten». I: *Tidsskrift for Rettsvitenskap*. Årg. 117, nr. 4-5, s. 465–498.

Green, Harold P. (1956): «Information Control and Atomic Power Development». I: *Law and Contemporary Problems*. Årg. 21, nr. 1, s. 91–112.

Grepperud, Sverre (2009): «Kvalitet i helsetjenesten – hva menes egentlig?» [Kronikk]. I: *Tidsskrift for Den norske legeforening*. Årg. 129, nr. 11, s. 1112–1114.

Grimsmo, Anders (2007): «Medisinskfaglig analyse av behovet for enklere kommunikasjon i tilknytning til bruken av elektronisk pasientjournal». Trondheim, Norsk senter for elektronisk pasientjournal.

Grimsmo, Anders, Arild Faxvaag, og Hallvard Lærum (2007): «Prosesstøttende EPJ systemer – bakgrunn, definisjon og målsetninger», Norsk senter for elektronisk pasientjournal. (Rapport fra Nasjonal IKT's EPJ-fagforum).

The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), OECD, 23. september 1980.

Gunderssen, Ragnhild Bassøe (2005): «Realisering av innsyns- og informasjonsrettigheter ved et sykehjem». Hovedfagsoppgave, Universitet i Oslo, Avdeling for forvaltningsinformatikk.

Haave, Per (2007): «Da legene skulle autoriseres». I: *Tidsskrift for Den norske lægeforening*. Årg. 127, nr. 24, s. 3267–3271.

Hanssen, Gro Sandkjær, Leif Arne Heløe, og Jan Erling Klausen (2004): «Statlig tilsyn med kommunesektoren». Oslo, Norsk institutt for by- og regionforskning. (NIBR-rapport 2004:04), s. 114.

Hansson, Sven Ove (2002): «Kan moralfilosofin hantera riskproblemen?». I: Boholm, Åsa, Sven Ove Hansson, Johannes Persson og Martin Peterson (red.): *Osäkerhetens horisonter. Kulturella och etiska perspektiv på samhällets riskfrågor* Nora: Nya Doxa. s. 53–67.

Hart, H. L. A. (1961): *The Concept of Law*. Oxford: Clarendon Press.

Hartvigsen, Gunnar, Monika A. Johansen, Per Hasvold, Johan Gustav Bellika, Eirik Arsand, Eli Arild, Deede Gammon, Sture Pettersen, og Steinar Pedersen (2007): «Challenges in Telemedicine and eHealth: Lessons Learned from 20 Years with Telemedicine in Tromsø». (Konferanseartikkel presentert på Medinfo 2007 – the 12th World Congress on Health (medical) Informatics).

Hassol, Andrea, James M. Walker, David Kidder, Kim Rokita, David Young, Steven Pierdon, Deborah Deitz, Sarah Kuck, og Eduardo Ortiz (2004): «Patient experiences and attitudes about access to a patient electronic health care record and linked web messaging». I: *Journal of the American Medical Informatics Association*. Årg. 11, nr. 6, s. 505–513.

Heier, Jan R., Michael T. Dugan, og David L. Sayers (2005): «A century of debate for internal controls and their assessment: a study of reactive evolution». I: *Accounting History*. Årg. 10, nr. 3, s. 39–70.

Helsedirektoratet: «Pandemi – Myndighetenes nettside om pandemisk influensa» *http://www.pandemi.no/* [Lesedato: 14.04.2010].

Helsetilsynet: «Mangelfull tilgangsstyring til elektronisk pasientjournal truer taushetsplikten i sykehus (Brev til Helse- og omsorgsdepartementet)» *http://www.helsetilsynet.no/templates/LetterWithLinks____9430.aspx* [Lesedato: 14.04. 2010].

Herrestad, Henning (1996): *Formal theories of rights*. Oslo: Juristforbundets forlag.

Hohfeld, Wesley Newcomb (1913): «Some Fundamental Legal Conceptions as Applied in Judicial Reasoning». I: *Yale Law Journal*. Årg. 23, nr. 1, s. 16–59.

Holmes, Oliver Wendell (1897): «The Path of the Law». I: *Harvard Law Review*. Årg. 10, nr. 8, s. 457–478.

Hu, Vincent C., David F. Ferraiolo, og D. Richard Kuhn (2006): «Assessment of access control systems». Interagency Report 7316, U.S. Department of Commerce, National Institution of Standards and Technology.

Hudson, Barbara (2001): «Human Rights, Public Safety and the Probation Service: Defending Justice in the Risk Society». I: *The Howard Journal*. Årg. 40, nr. 2, s. 103–113.

Husom, Nina (2002): «Helsevesenet trenger en medisinsk havarikommisjon» [Nyheter og reportasjer]. I: *Tidsskrift for Den norske legeforening*. Årg. 122, nr. 12, s. 1238.

Hvordan holde orden i eget hus: Internkontroll i sosial- og helsetjenesten (2009). Bestillingsnummer IS-1183. Oslo, Helsedirektoratet. (Veilder. Først utgitt i 2004), s. 36.

Høgberg, Alf Petter, og Marius Stub (2009): «Er reglene om bruk av tvangsmidler i avvergende og forebyggende øyemed forenelige med forbudet mot husinkvisisjoner i Grunnloven § 102?». I: *NOU 2009:15, Skjult informasjon – åpen kontroll.* Vedlegg 3, s. 420–449.

Internal Control – Integrated Framework (1992), COSO (The Committee of Sponsoring Organizations of the Treadway Commission).

Internkontroll i barneverntjenesten i kommunene – en veileder (2006). Q-1105 B. Oslo, Barne- og likestillingsdepartementet. (Veilder), s. 24.

Johansen, Kjell, og Leiv S. Bakketeig (1979): «Erfaringer med bruk av skjema for svangerskapskontroll». I: *Tidsskrift for Den norske lægeforening*. Årg. 99, nr. 7, s. 389–391.

Jones, Andrew J. I., og Marek Sergot (1992): «Deontic logic in the representation of law: Towards a methodology». I: *Artificial Intelligence and Law*. Årg. 1, nr. 1, s. 45–64.

——— (1996): «A Formal Characterisation of Institutionalised Power». I: *Logic Journal of the IGPL*. Årg. 4, nr. 3, s. 427–443.

Jøldal, Bjørn (1972): «Narkotikaforskrivning og forbruk i Norge». I: *Tidsskrift for Den norske lægeforening*. Årg. 92, nr. 27, s. 1809–1811.

Jøldal, Bjørn, og Tullik Halvorsen (1972): «Electronic data processing in the control of legal consumption of narcotics in Norway». I: *Bulletin on Narcotics (United Nations dept. of Social Affairs)*. Årg. 24, nr. 1, s. 55–57.

Kaasen, Knut (1981): «Norske myndigheters kontroll med sikkerheten i petroleumsvirksomheten på norsk kontinentalsokkel». I: *Tidsskrift for Rettsvitenskap*. Årg. 92, nr. 1, s. 82–103.

Karanja, Stephen Kabera (2008): *Transparency and proportionality in the Schengen Information System and border control co-operation*. Leiden: Nijhoff. [Først utgitt som dr. juris avhandling, Oslo 2006].

Karjoth, Günter, Matthias Schunter, og Michael Waidner (2003): «Platform for Enterprise Privacy Practices: Privacy-Enabled Management of Customer Data». I: Dingledine, Roger og Paul Syverson (red.): *Privacy enhancing technologies : second international workshop, PET 2002, San Francisco, CA, USA, April 14-15, 2002 : revised papers*. San Francisco, CA, USA: Springer. s. 194–198.

Kc, Gaurav S., og Paul A. Karger. «Preventing Attacks on Machine Readable Travel Documents (MRTDs).» *IBM Research Report* (2006).

Kindt, Olaf Trampe (1952): «Lægens taushetsplikt». I: *Norsk retstidende*. Årg. 117, s. 961–967.

——— (1957): «Fremleggelse av sykejournaler som bevis i rettssak». I: *Norsk retstidende*. Årg. 122, s. 129–135.

KITH: «Kodeverk og terminologi» *http://www.kith.no/samfunnsoppgaver/kodeverk_og_terminologi* [Lesedato: 14.04.2010].

Kjeldstadli, Knut (1999): *Fortida er ikke hva den en gang var*. 2. utgave. Oslo: Universitetsforlaget. [1. utgave 1992].

Kjønstad, Asbjørn (1978): «Sosialarbeidernes taushetsplikt». I: *Lov og Rett*. Årg. 17, s. 491–509.

——— (1982): «Pasienters rettigheter – kontraktsrett eller forvaltningsrett?». I: Bratholm, Anders, Nils Christie og Torkel Opsahl (red.): *Lov og frihet: festskrift til Johs. Andenæs på 70-årsdagen*. Oslo: Universitetsforlaget. s. 587–602.

——— (2005): «Styringsretten i helsevesenet». I: *Arbeidsrett*. Årg. 2, nr. 1, s. 1–27.

——— (2007): *Helserett: pasienters og helsearbeideres rettsstilling*. 2. utgave. Oslo: Gyldendal akademisk. [1. utgave 2005].

KOM(2004) 356. «E-sundhed – et bedre sundhedsvæsen for Europas borgere: En handlingsplan for et europæisk e-sundhedsområde». (Bruxelles, Kommisionen for de europæiske fællesskaber).

KOM(2007) 651. «Meddelelse fra kommisionen om øget sprængstofsikkerhed». (Bruxelles, Kommissionen for de europæiske fællesskaber).

KOM(2008) 414. «Forslag til Europa-parlamentets og rådets direktiv om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser». (Bruxelles, Kommissionen for de europæiske fellesskaber).

Knoph, Ragnar (1948): *Rettslige standarder: særlig Grunnlovens § 97*. Oslo: I kommisjon hos Grøndahl. [Først utgitt i 1939, posthumt].

Knudsen, Morten. «En guide til litteratur om metode, analysestrategi og videnskabsteori». Working paper No. 2009.01, Copenhagen Business School, Institut for organisation. 2009.

Kolstad, Per, og Kjell Nordbye (1971): «Et system for automatisk databehandling av medisinske journaler». I: *Tidsskrift for Den norske lægeforening*. Årg. 91, nr. 6, s. 405–409.

Krogh, Christen (1997): *Normative structures in natural and artificial systems*. Oslo: Tano-Aschehoug.

Krogh, Christen, og Henning Herrestad (1999): «Hohfeld in cyberspace and other applications of normative reasoning in agent technology». I: *Artificial Intelligence and Law*. Årg. 7, nr. 1, s. 81–96.

Kvalitet i pleie- og omsorgstjenestene (2004). Bestillingsnummer: IS-1201. Oslo, Sosial- og helsedirektoratet. (Veileder).

Landwehr, Carl E., Alan R. Bull, John P. McDermott, og William S. Choi (1994): «A taxonomy of Computer Program Security Flaws». I: *ACM computing surveys*. Årg. 26, nr. 3, s. 211–254.

Larssen, Vetle Lid (2007): *Norske helter* [Roman]. Oslo: Cappelen.

Latour, Bruno (1996): «Social theory and the study of computerized work sites». I: Orlikowski, Wanda J., Geoff Walsham, Matthew R. Jones og Janice I. DeGross (red.): *Information technology and changes in organizational work*. London: Chapman & Hall. s. 295–307.

Lessig, Lawrence (1999): *Code and other laws of cyberspace*. New York: Basic Books.

Light, Donald W., og Olaf Gjerløw Aasland (2003): «Den nye legerollen – kvalitet, åpenhet og tillit» [Kronikk]. I: *Tidsskrift for Den norske legeforening*. Årg. 123, nr. 13/14, s. 1870–1873.

Lindahl, Lars (1977): *Position and change: a study in law and logic*. Dordrecht: D. Reidel.

——— (2004): «Deduction and Justification in the Law. The Role of Legal Terms and Concepts». I: *Ratio Juris*. Årg. 17, nr. 2, s. 182–202.

——— (2005): «Hohfeld relations and spielraum for action». I: Dahlman, Christian (red.): *Studier i rättsekonomi. Festskrift till Ingemar Ståhl*. Lund: Studentlitteratur. s. 121–150.

Lindbekk, Tore (1992): «The Weberian Ideal-type: Development and Continuities». I: *Acta Sociologica*. Årg. 35, nr. 4, s. 285–297.

Lloyd-Bostock, Sally M., og Bridget M. Hutter (2008): «Reforming regulation of the medical profession: The risks of risk-based approaches». I: *Health, Risk & Society*. Årg. 10, nr. 1, s. 69–83.

Løyning, Trond (2005): «Kredittilsynet i en neoliberal økonomi : finansmarkedenes dannelse». I: *Sosiologisk tidsskrift*. Årg. 13, nr. 4, s. 335–362.

Makinson, David (1986): «On the formal representation of rights relations». I: *Journal of philosophical Logic*. Årg. 15, nr. 4, s. 403–425.

Materstvedt, Lars Johan, og Aslak Syse (2006): «Døendes rettsstilling» [Debattartikkel]. I: *Tidsskrift for Den norske lægeforening*. Årg. 126, nr. 4, s. 488–489.

Matten, Dirk, og Andrew Crane (2005): «What is stakeholder democracy? Perspectives and issues». I: *Business Ethics: A European Review*. Årg. 14, nr. 1, s. 6–13.

McCarty, L. Thorne (1989): «A language for legal Discourse I. basic features». (Konferanseartikkel presentert på 2nd international conference on Artificial Intelligence and Law).

Midttun, Linda, Erik Sverrbo, Glen Thorsen, og Olafr Steinum (2003): «Er det sammenfall mellom journalopplysninger og innrapporterte data? En studie av 500 pasientopphold ved norske somatiske sykehus i 2001». STF78 A035504. Trondheim, Sintef.

MinJournal: «MinJournal – på nett med helsevesenet» *http://www.minjournal.no* [Lesedato: 14.04.2010].

Mjaaland, Marianne (2003): *Unaturlig dødsfall meldes* [Roman]. Oslo: Gyldendal.

Mjåset, Christer (2008): *Legen som visste for mye* [Roman]. Oslo: Gyldendal.

Moland, Leif E. (2005): «Med legene på laget: Et fagutviklingsprogram for å utvikle legenes rolle i et inkluderende arbeidsliv». Fafo-notat 2005:06. Oslo, Fafo. (Følgeforskning Inkluderende arbeidsliv).

Moody, Harry R. (1988): «From Informed Consent to Negotiated Consent». I: *The Gerontologist*. Årg. 28, s. 64–70.

Nessa, John (2000): «Diagnosar drep – og gjer frisk» [Essay]. I: *Utposten*. Årg. 29, nr. 1, s. 4–7.

Nordby, Trond (1993): «Det offentlige helsevesenet – en fagstyrets høyborg». I: Nordby, Trond (red.): *Arbeiderpartiet og planstyret 1945–1964*. Oslo: Universitetsforlaget. s. 105–120.

Norm for informasjonssikkerhet i helsesektoren – Datatilsynets vurdering (2006), Datatilsynet. (Brev til Sosial- og helsedirektoratet 7. august 2006).

Nystadnes, Torbjørn (2007a): «EPJ Standard del 1: Introduksjon til EPJ standard». Trondheim. (KITH-rapport nr. 5/05).

——— (2007b): «EPJ Standard del 2: Tilgangsstyring, redigering, retting og sletting». Trondheim. (KITH-rapport nr. 6/05).

Ohnstad, Bente (1991): «Taushetsplikt og utlevering av pasientjournal». I: *Tidsskrift for Den norske lægeforening*. Årg. 111, nr. 18, s. 2317–2319.

——— (2006): «Medisinsk forskning og jus» [Bokanmeldelse]. I: *Tidsskrift for Den norske legeforening*. Årg. 126, nr. 10, s. 1366–1367.

Olsen, Thomas (2009): «Personvernøkende identitetsforvaltning» Manuskript innlevert til bedømmelse for Phd-graden ved Det juridiske fakultet, UiO, 24. september 2009. Avdeling for forvaltningsinformatikk, Juridisk fakultet, Universitetet i Oslo.

Olsen, Thomas, og Tobias Mahler (2007): «Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II». I: *Computer Law & Security Report*. Årg. 23, nr. 5, s. 415–426.

Omveien, Thale (2010): *Tribus Lingua – håndbok i teknokratsjargong*. n'te utgave. Storevik: Falsum forlag.

Parker, Christine (2008): «The Pluralization of Regulation». I: *Theoretical Inquiries in Law*. Årg. 9, nr. 2, s. 349–369.

Pasientjournalen : innhold, gruppering og arkivering av pasientdokumentasjon i somatiske sykehus (1994). (Statens helsetilsyns utredningsserie; 1994:3).

Pedersen, Reidar, Bjørn Hofmann, og Margrete Mangset (2007a): «Pasientautonomi og informert samtykke i klinisk arbeid» [Oversiktsartikkel]. I: *Tidsskrift for Den norske legeforening*. Årg. 127, nr. 12, s. 1644–1647.

Pedersen, Reidar, Marianne Klungland Bahus, og Erik Martinsen Kvisle (2007b): «Behandlingsunnlatelse, etikk og jus». I: *Tidsskrift for Den norske legeforening*. Årg. 127, nr. 12, s. 1648–1650.

Personvernombud. Ombudets rolle og arbeidsoppgaver (2007). Oslo, Datatilsynet. (Veileder).

Petković, Milan, Stefan Katzenbeisser, og Klaus Kursawe (2007): «Rights Management Technologies: A Good Choice for Securing Electronic Health Records?». I: Pohlmann, Norbert, Helmut Reimer og Wolfgang Schneider (red.): *ISSE/SECURE 2007 Securing Electronic Business Processes*. s. 178–187.

Povey, Dean (1999): «Optimistic security: a new access control paradigm». (Konferanseartikkel presentert på the 1999 workshop on New Security Paradigms) Ontario, Canada.

Power, Michael (2004): *The Risk Management of Everything: Rethinking the Politics of Uncertainty*. London: Demos.

Pseudonyme helseregistre, rundskriv fra Helse- og omsorgsdepartementet (2005). I-2005-8 (helseregisterloven § 8).

Quist, Arvin S. (2002): *Security Classification of Information: Introduction, History, and Adverse Impacts*. 2. utgave. Oak Ridge, Tennessee, USA: Oak Ridge Classification Associates. [1. utgave 1989].

Rapport fra tilsyn med konfidensialiteten og tilgjengeligheten til elektronisk pasientjournal ved Akershus universitetssykehus HF (2006). 6. og 7. juni 2006, Helsetilsynet i Oslo og Akershus, Statens helsetilsyn og Datatilsynet. (Rapport fra felles tilsyn).

Rapport frå tilsyn med informasjonstryggleiken ved pasientjournalsystemet Doculive og det pasientadministrative systemet PIMS ved Helse Bergen HF, Haukeland universitetssjukehus (2006). 5. og 6. mai 2006, Helsetilsynet i Hordaland, Statens helsetilsyn og Datatilsynet.

Rasmussen, Ørnulf (1997): *Kommunikasjonsrett og taushetsplikt i helsevesenet*. Ålesund: A.S. Borgund.

Ravlum, Inger-Anne (2005): «Setter vår lit til Storebror … og alle småbrødre med?: Befolkningens holdning til og kunnskap om personvern». TØI-rapport 789/2005. Oslo, Transportøkonomisk institutt.

Rawls, John (1999): *A Theory of Justice*. Revidert utgave. Oxford: Oxford University Press. [1. utgave 1971].

Reidenberg, Joel R. (1998): «Lex informatica: The formulation of information policy rules through technology». I: *Texas Law Review*. Årg. 76, nr. 3, s. 553–584.

Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens (1973), U.S. Department of Health, Education and Welfare.

Retningslinjer for kvalitetsutvalgenes oppgaver, funksjon og sammensetning (1994). Oslo, Statens helsetilsyn. (Vedlegg til statens helsetilsyns rundskriv av 4. februar 1994, IK-7/94).

Riksrevisjonens undersøkelse av kodekvaliteten ved helseforetakene (2006). Dokument nr. 3:7 (2005-2006).

Risikovurdering av informasjonssystem med utgangspunkt i forskrift til personopplysningsloven (2002). TV-506:2002. Oslo, Datatilsynet. (Veileder).

Ritchie, Lisa (2007): «Evaluation of a patient-held record for Meticillin Resistant Staphylococcus Aureus (MRSA)». I: *British Journal of Infection Control*. Årg. 8, nr. 4, s. 25–29.

Rock, Ellen M., og Patricia S. Simmons (2003): «Physician knowledge and attitudes of Minnesota laws concerning adolescent health care». I: *Journal of pediatric and adolescent gynecology*. Årg. 16, nr. 2, s. 101–108.

Rooksby, John, og Stephen Kay (2001): «Clinical narrative and clinical organisation: Properties of radiology reports». I: Patel, V.L., R. Rogers og R. Haux (red.): *Medinfo 2001. Studies in health technology and informatics*: IOS Press. s. 680–684.

Ross, Alf (1953): *Om ret og retfærdighed: en indførelse i den analytiske retsfilosofi*. København: Nyt Nordisk Forlag.

——— (1957): «Tû-tû». I: *Harvard Law Review*. Årg. 70, nr. 5, s. 812–825.

Ross, Stephen E., og Chen-Tan Lin (2003): «The effects of promoting patient access to medical records: a review». I: *Journal of the American Medical Informatics Association*. Årg. 10, nr. 2, s. 129–138.

Rundskriv vedrørende tilgang til og utlevering av opplysninger i elektroniske pasientjournaler (2006). IS-7/2006, Sosial- og helsedirektoratet.

Røst, Thomas Brox, Øystein Nytrø, og Anders Grimsmo (2006): «Classifying Encounter Notes in the Primary Care Patient Record». (Konferanseartikkel presentert på 3rd International Workshop on Text-based Information Retrieval, TIR-06).

Røstad, Lillian (2006): «An extended misuse case notation: Including vulnerabilities and the insider threat». (Konferanseartikkel presentert på The Twelfth International Working Conference on Requirements Engineering: Foundation for Software Quality).

——— (2007): «MG-RBAC: Using Medical Guidelines as a Source of Contextual Information to Activate and Deactivate Roles and Permissions». (Konferanseartikkel presentert på MedInfo 2007, the 12th World Congress on Health (Medical) Informatics) Brisbane, Australia.

Røstad, Lillian, og Øystein Nytrø (2008): «Personalized access control for a personally controlled health record». (Konferanseartikkel presentert på the 2nd ACM workshop on Computer security architectures) Alexandria, Virginia, USA.

Saltzer, Jerome H, og Michael D Schroeder (1975): «The Protection of Information in Computer Systems». I: *Proceedings of IEEE*. Årg. 63, nr. 9, s. 1278–1308.

Samarati, Pierangela, og Latanya Sweeney (1998): «Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression», Computer Science Laboratory, SRI International. (Technical Report, SRI-CSL-98-04), s. 384–393.

Sand, Inger-Johanne (2005): «Retten i det polykontekstuelle samfunn. Hvordan skal vi analysere og forstå den?». I: *Retfærd. Nordisk Juridisk Tidsskrift*. Årg. 28, nr. 4, s. 1–28.

Sandgren, Claes (2007): «Framtidens doktorsavhandlingar i rättsvetenskap». I: *Tidsskrift for Rettsvitenskap*. Årg. 120, nr. 3, s. 388–407.

Sandhu, Ravi S., Edward J. Coyne, Hal L. Feinstein, og Charles E. Youman (1996): «Role-based access control models». I: *IEEE computer*. Årg. 29, nr. 2, s. 38–47.

Sartor, Giovanni (2006): «Privacy, Reputation, and Trust: Some Implications for Data Protection». I: Stølen, Ketil (red.): *Trust Management*. Berlin: Springer. s. 354–366.

——— (2009): «Legal concepts as inferential nodes and ontological categories». I: *Artificial Intelligence and Law*. Årg. 17, nr. 3, s. 217–251.

Sauter, Wolf (2009): «The Proposed Patients' Rights Directive and the Reform of (Cross-Border) Healthcare in the European Union». I: *Legal issues of economic integration*. Årg. 36, nr. 2, s. 109–131.

Scharling, Sven, Søren Mayland, og Maria Becher Trier (2007): «Undersøgelse om forholdet mellem tavshedspligt og indberetningspligt». Danmark, Scharling Research.

Schartum, Dag Wiese (1993): *Rettssikkerhet og systemutvikling i offentlig forvaltning*. Oslo: Universitetsforlaget.

——— (2005): «Utvikling av beslutningssystemer – fra lovtekst til programkode». Forvaltningsinformatisk notatserie, 1/2005, Universitetet i Oslo, Avdeling for forvaltningsinformatikk.

Schartum, Dag Wiese, og Lee A. Bygrave (2004): *Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger*. Bergen: Fagbokforlaget.

——— (2006): «Utredning av behov for endringer i personopplysningsloven: skrevet etter oppdrag fra Justisdepartementet og Moderniseringsdepartementet». Oslo, Justis- og politidepartementet.

Schroeder, Christopher H. (1986): «Rights against Risks». I: *Columbia Law Review*. Årg. 86, nr. 3, s. 495–562.

Scott, Colin (2003): «Speaking Softly Without Big Sticks: Meta-Regulation and Public Sector Audit». I: *Law & Policy*. Årg. 25, nr. 3, s. 203–219.

Selmer, Knut S. (1977): «Medisinske informasjonssystemer – en utfordrende blanding av velsignelser og farer». I: Blekeli, Ragnar Dag og Knut S. Selmer (red.): *Data og personvern*. Oslo: Universitetsforlaget. s. 117–132.

Senter for rettsinformatikk: «Forskningsområder, rettsteknologi». Institutt for privatrett, Juridisk fakultet, Universitetet i Oslo, *http://www.jus.uio.no/ifp/forskning/omrader/rettsinformatikk-og-eforvaltning/rettsteknologi/* [Lesedato: 14.04.2010].

Sheppard, Nicholas Paul, Reihaneh Safavi-Naini, og Mohammad Jafari (2009): «A Digital Rights Management Model for Healthcare». (Konferanseartikkel presentert på IEEE International Symposium on Policies for Distributed Systems and Networks).

Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer (2000). SV-100:2000. Oslo, Datatilsynet.

Simborg, Donald W. (1981): «DRG creep: a new hospital-acquired disease». I: *New England Journal of Medicine*. Årg. 304, nr. 26, s. 1602–1604.

Simonsen, Sigmund, og Magne Nylenna (2005): *Helseforskningsrett: den rettslige regulering av medisinsk og helsefaglig forskning*. Oslo: Gyldendal akademisk.

SINTEF: «iAccess informasjonsside» *http://www.sintef.no/Informasjons--og-kommunikasjonsteknologi-IKT/Systemutvikling-og-sikkerhet/Prosjekter/iAccess/* [Lesedato: 14.04.2010].

Skidmore, Paul, Jake Chapman, og Paul Miller (2003): *The Long Game. How Regulators and Companies Can Both Win*. London: Demos.

Slagstad, Rune (2009): «Styringsvitenskap – ånden som går». I: *Nytt Norsk Tidsskrift*. Årg. 26, nr. 3-4, s. 411–434.

Sloman, Morris (1994): «Policy driven management for distributed systems». I: *Journal of network and Systems Management*. Årg. 2, nr. 4, s. 333–360.

Solhaug, Bjørnar, Dag Elgesem, og Ketil Stølen (2007): «Specifying Policies Using UML Sequence Diagrams – An Evaluation Based on a Case Study». (Konferanseartikkel presentert på POLICY '07. Eighth IEEE International Workshop on Policies for Distributed Systems and Networks) Bologna, Italy.

Spira, Laura F., og Michael Page (2003): «Risk Management: The Reinvention of Internal Control and the Changing Role of Internal Audit». I: *Accounting, Auditing & Accountability Journal*. Årg. 16, nr. 4, s. 640–661.

Stefik, Mark (1997): «Shifting the possible: How trusted systems and digital property rights challenge us to rethink digital publishing». I: *Berkeley Technology Law Journal*. Årg. 12, s. 137–159.

Steihaug, Sissel, Trond Harsvik, Jan-W. Lippestad, og Nils Bringager (2008): «Kartlegging og risikovurdering av HMS i hjemmetjenesten i bydelene Oslo kommune». Trondheim/Oslo, Sintef Helse.

Stenvik, Are (2003): «Rettsbeskyttelse av personlig særpreg». I: *Tidsskrift for Rettsvitenskap*. Årg. 116, nr. 5, s. 601–647.

Stewart, Irvin (1948): *Organizing scientific research for war: The administrative history of the Office of Scientific Research and Development*: Little, Brown and Company.

Stone, Christopher D. (1975): *Where the Law Ends: The social control of corporate behavior*. New York: Harper & Row.

——— (1985): «Corporate Social Responsibility: What It Might Mean, If It Were Really to Matter» [Essay]. I: *Iowa Law Review*. Årg. 71, nr. 2, s. 557–575.

Svarlien, Astrid Brevik (2008): «Forprosjektet Elektronisk Helsekort for gravide (EHG) – Forslag til løsning og plan for hovedprosjekt». (KITH-rapport nr. 24/08).

Sviktende tilgangsstyring i elektroniske pasientjournaler? Lovforslag om å tillate direkte tilgang til pasientjournaler på tvers av virksomhetsgrensene (2009), Datatilsynet. (Rapport april 2009).

Syse, Aslak (2009): *Pasientrettighetsloven. Med kommentarer*. 3. utgave. Oslo: Gyldendal Akademisk. [1. utgave 2001].

Teubner, Günther (1983): «Substantive and Reflexive Elements in Modern Law». I: *Law and Society Review*. Årg. 17, nr. 2, s. 239–285.

——— (1985): «Corporate Fiduciary Duties and Their Beneficiaries: A Functional Approach to the Legal Institutionalization of Corporate Responsibility». I: Hopt, Klaus J. og Günther Teubner (red.): *Corporate Governance and Directors' Liabilities. Legal, Economic and Sociological Analyses on Corporate Social Responsibilities*. Berlin: Walter de Gruyter.

Thomas, R. L., og Robert H. Courtney (1974): «A Systematic Approach to Data Security». (Konferanseartikkel presentert på Approaches to privacy and security in computer systems: a conference held at the National Bureau of Standards, March 4-5, 1974) Washington D.C.

Tilsyn med helsepersonell og helsevesen basert på informasjon om enkelthendelser mv. – Rettslige rammer (2004). Oslo, Helsetilsynet. (Helsetilsynet – Styrende dokument).

Tilsyn med kodepraksis (2004). Rapport fra Helsetilsynet.

Torgersen, Ulf (1972): *Profesjonssosiologi*. Oslo: Universitetsforlaget.

Tranvik, Tommy (2009): *Personvern og informasjonssikkerhet. En studie av rettsreglers etterlevelse i kommunal sektor*. Complex 4/09. Oslo: Senter for rettsinformatikk.

Tranøy, Bent Sofus (2000): «Losing credit. The politics of liberalisation and macro-economic regime change in Norway 1980-92 (99)», The Department of Political Science, University of Oslo.

Tranøy, Knut Erik (2005): *Medisinsk etikk i vår tid*. 4. utgave. Bergen: Fagbokforlaget. [1. utgave: Søreidgrend, Sigma, 1991].

Tuerkheimer, Frank M. (1993): «The underpinnings of privacy protection». I: *Communications of the ACM*. Årg. 36, nr. 8, s. 69–73.

Turing, Alan M. (1950): «I.–Computing Machinery and Intelligence». I: *Mind*. Årg. LIX, nr. 236, s. 433–460.

Tønnesson, Johan L. (2001): *Vitenskapens stemmer*. Oslo: Norsk faglitterær forfatter- og oversetterforening.

Urettmessig påføring av legereservasjon i apotek (2005), Den norske lægeforening. (Brev til Helse- og omsorgsdepartementet 14. desember 2005).

Vedvik, Eivind, og Arild Faxvaag (2006): «The fate of clinical department systems at the dawn of hospital-wide electronic health records in a Norwegian university hospital». I: *Studies in health technology and informatics*. nr. 124, s. 298–303.

von Wright, Georg Henrik (1999): «Deontic Logic: A Personal View». I: *Ratio Juris*. Årg. 12, nr. 1, s. 26–38.

Vurdering av risiko for voldelig atferd: bruk av strukturerte kliniske verktøy (2007). Bestillingsnummer IS-9/2007. Oslo, Sosial- og helsedirektoratet, Avdeling psykisk helse. s. 11.

Wartofsky, Marx W. (1979): *Models: representation and the scientific understanding*. Dordrecht: D. Reidel Pub Co.

Weber, Max (1994): «Objectivity and understanding in economics». I: Hausman, Daniel M. (red.): *The philosophy of economics: An anthology*, Second Edition: Cambridge University Press, [Oversatt utdrag fra «Die 'Objektivität' sozialwissenschaftlicher und sozialpolitischer Erkenntnis», først utgitt i 1904]. s. 69–82.

Weed, Lawrence L. (1968): «Medical records that guide and teach». I: *New England Journal of Medicine*. Årg. 278, nr. 11 og 12, s. 593–600 og 652–657.

——— (2006): «Idols of the Mind». (Konferanseartikkel presentert på 7th Annual International Summit on Redesigning the Clinical Office Practice [Plenary session paper]) San Diego, USA.

Weitzner, Daniel J., Harold Abelson, Tim Berners-Lee, Joan Feigenbaum, James Hendler, og Gerald Jay Sussman (2008): «Information accountability». I: *Communications of the ACM*. Årg. 51, nr. 6, s. 82–87.

Westin, Alan F. (1967): *Privacy and freedom*. New York: Atheneum.

Wikse, Kari Anne (1995): «Taushetsplikten - hva og hvordan: har sykepleiere nok faglig kunnskap til å ivareta tillit og respekt mellom pasient og sykepleier når edb-baserte pasientjournaler innføres? : en teoretisk studie», Institutt for sykepleievitenskap, Universitetet i Oslo.

Wildavsky, Aaron (1988): *Searching for safety*. New Brunswick, N.J.: Transaction Books.

Wilensky, Harold L. (1964): «The Professionalization of Everyone?». I: *The American Journal of Sociology*. Årg. 70, nr. 2, s. 137–158.

Witty, Roberta J., Ant Allan, John Enck, og Ray Wagner. «Identity and Access Management Defined.» *Gartner Research* (2003).

Working Document on the processing of personal data relating to health in electronic health records (EHR) (2007). 00323/07/EN WP 131, Article 29 Data Protection Working Party. (Working Documents).

World Health Organization: «History of ICD» *http://www.who.int/classifications/icd/en/* [Lesedato: 14.04.2010].

World Medical Association: «Declaration of Helsinki: Ethical Principles for Research Involving Human Subjects» *http://www.wma.net/en/30publications/10policies/b3/index.html* [Lesedato: 14.04.2010].

Zapffe, Peter Wessel (1996): *Om det tragiske*. Oslo: Pax. [1. utgave: Gyldendal, 1941].

Østerud, Øyvind, Fredrik Engelstad, og Per Selle (2003): *Makten og demokratiet: en sluttbok fra Makt- og demokratiutredningen*. Oslo: Gyldendal akademisk.

Øyen, Else (1980): «Rammen om taushetsplikten». I: Kjønstad, Asbjørn og Else Øyen (red.): *Taushetsplikt i sosialsektoren*. Bergen: Universitetsforlaget. s. 75–111.

Aasen, Henriette Sinding (2000): *Pasientens rett til selvbestemmelse ved medisinsk behandling*. Bergen: Fagbokforlaget.

——— (2008): «Barns rett til selvbestemmelse og medbestemmelse i beslutninger om helsehjelp». I: *Tidsskrift for familierett, arverett og barnevernrettslige spørsmål*. Årg. 6, nr. 1, s. 4–27.

Aaslestad, Petter (2007): *Pasienten som tekst: fortellerrollen i psykiatriske journaler. Gaustad 1890-1990*. 2. utgave. Oslo: Universitetsforlaget. [1. utgave 1997].

B: Lover, forskrifter og annet særskilt regelverk

Norske lover

Lov 17. mai 1814. Kongeriget Norges Grundlov, given i Rigsforsamlingen paa Eidsvold den 17de Mai 1814 (Grunnloven).

Lov 17. august 1848. Lov om Sindssyges Behandling og Forpleining (sinnsykeloven). *[Opphevet]*.

Lov 16. mai 1860. Lov om Sundhedscommissioner og om Foranstaltninger i Anledning af epidemiske og smitsomme Sygdomme (sundhedsloven). *[Opphevet]*.

Lov 1. juli 1887 nr. 5. Lov om Rettergangsmaaden i Straffesager (straffeprosessloven). *[Opphevet]*.

Lov 22. mai 1902 nr. 10. Almindelig borgerlig Straffelov (straffeloven).

Lov 9. juni 1903 nr. 7. Lov om Statskontrol med Skibes Sjødygtighed m.v. (sjødygtighedsloven). *[Opphevet]*.

Lov 29. april 1927 nr. 1. Lov om lægers rettigheter og plikter (legeloven). *[Opphevet]*.

Lov 7. desember 1956 nr. 2. Lov om arbeidervern (arbeidervernloven). *[Opphevet]*.

Lov 10. februar 1967. Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven).

Lov 19. juni 1969 nr. 57. Lov om sykehus m.v. (sykehusloven). *[Opphevet]*.

Lov 21. mai 1971 nr. 47. Lov om brannfarlige varer samt væsker og gass under trykk [gjelder bare for Svalbard] (brannfarlighetsloven (Svalbard)). *[erstattet av lov 14. juni 2002 nr. 20, gjelder nå bare for Svalbard]*.

Lov 14. juni 1974 nr. 39. Lov om eksplosive varer (lov om eksplosive varer (Svalbard)). *[erstattet av lov 14. juni 2002 nr. 20, gjelder nå bare for Svalbard]*.

Lov 11. juni 1976 nr. 79. Lov om kontroll med produkter og forbrukertjenester (produktkontrolloven).

Lov 4. februar 1977 nr. 4. Lov om arbeidervern og arbeidsmiljø m.v. (arbeidsmiljøloven). *[Opphevet]*.

Lov 9. juni 1978 nr. 48. Lov om personregistre m.m. (personregisterloven). *[Opphevet]*.

Lov 13. juni 1980 nr. 42. Lov om leger (legeloven). *[Opphevet]*.

Lov 13. mars 1981 nr. 6. Lov om vern mot forurensninger og om avfall (forurensningsloven).

Lov 19. november 1982 nr. 66. Lov om helsetjenesten i kommunene (kommunehelsetjenesteloven).

Lov 30. mars 1984 nr. 15. Lov om statlig tilsyn med helsetjenesten (helsetilsynsloven).

Lov 22. mars 1985 nr. 11. Lov om petroleumsvirksomhet (petroleumsloven). *[Opphevet]*.

Lov 5. juni 1987 nr. 26. Lov om brannvern (brannvernloven). *[Opphevet]*.

Lov 16. juni 1989 nr. 69. Lov om forsikringsavtaler (forsikringsavtaleloven).

Lov 13. desember 1991 nr. 81. Lov om sosiale tjenester m.v. (sosialtjenesteloven).

Lov 17. juli 1992 nr. 100. Lov om barneverntjenester (barnevernloven).

Lov 16. juni 1994 nr. 20. Lov om tekniske kontrollorgan som har til oppgåve å gjennomføre samsvarsvurderingar (lov om tekniske kontrollorgan).

Lov 5. august 1994 nr. 55. Lov om vern mot smittsomme sykdommer (smittevernloven).

Lov 29. november 1996 nr. 72. Lov om petroleumsvirksomhet (petroleumsloven).

Lov 28. februar 1997 nr. 19. Lov om folketrygd (folketrygdloven).

Lov 20. mars 1998 nr. 10. Lov om forebyggende sikkerehtstjeneste (sikkerhetsloven).

Lov 21. mai 1999 nr. 30. Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven).

Lov 2. juli 1999 nr. 61. Lov om spesialisthelsetjenesten m.m. (spesialisthelsetjenesteloven).

Lov 2. juli 1999 nr. 62. Lov om etablering og gjennomføring av psykisk helsevern (psykisk helsevernloven).

Lov 2. juli 1999 nr. 63. Lov om pasientrettigheter (pasientrettighetsloven).

Lov 2. juli 1999 nr. 64. Lov om helsepersonell m.v. (helsepersonelloven).

Lov 14. april 2000 nr. 31. Lov om behandling av personopplysninger (personopplysningsloven).

Lov 12. mai 2000 nr. 36. Lov om strålevern og bruk av stråling (strålevernloven).

Lov 18. mai 2001 nr. 24. Lov om helseregistre og behandling av helseopplysninger (helseregisterloven).

Lov 21. februar 2003 nr. 12. Lov om behandlingsbiobanker (behandlingsbiobankloven).

Lov 27. juni 2003 nr. 64. Lov om alternativ behandling av sykdom mv. (alternativ behandlingsloven).

Lov 5. desember 2003 nr. 100. Lov om humanmedisinsk bruk av bioteknologi m.m. (bioteknologiloven).

Lov 17. juni 2005 nr. 62. Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven).

Lov 19. mai 2006 nr. 16. Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova).

Lov 16. juni 2006 nr. 20. Lov om arbeids- og velferdsforvaltningen (arbeids- og velferdsforvaltningsloven [«NAV-loven»]).

Lov 16. februar 2007 nr. 9. Lov om skipssikkerhet (skipssikkerhetsloven).

Lov 20. juni 2008 nr. 44. Lov om medisinsk og helsefaglig forskning (helseforskningsloven).

Lov 9. januar 2009 nr. 2. Lov om kontroll med markedsføring og avtalevilkår mv. (markedsføringsloven).

Lov 19. juni 2009 nr. 44. Lov om kommunale krisesentertilbod (krisesenterlova).

Lov 18. desember 2009 nr. 131. Lov om sosiale tjenester i arbeids- og velferdsforvaltningen (lov om sosiale tjenester i NAV).

Forskrifter

Forskrift 7. desember 1982 nr. 3442. Forskrift om internkontroll i bedrifter som tilvirker eller bearbeider brannfarlige varer (behandlingsbedrifter) (internkontrollforskrift brannfarlig vare).

[Opphevet. Opprinnelig gitt som retningslinje fra daværende tilsynsmyndighet; Statens sprengstoffinspeksjon].

Forskrift 22. mars 1991 nr. 159. Forskrift om internkontroll for miljø og sikkerhet (internkontrollforskriften). *[Opphevet]*.

Forskrift 15. desember 1994 nr. 1187. Forskrift om internkontroll for å oppfylle næringsmiddellovgivningen (internkontrollforskriften for næringsmidler).

Forskrift 6. desember 1996 nr. 1127. Forskrift om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (internkontrollforskriften).

Forskrift 20. juni 1997 nr. 1057. Forskrift om klargjøring av kontrollansvar, dokumentasjon og bekreftelse av den interne kontroll. (internkontrollforskrift finansinstitusjoner). *[Opphevet]*.

Forskrift 11. desember 1998 nr. 1193. Forskrift om offentlege arkiv (arkivforskrifta).

Forskrift 15. desember 2000 nr. 1265. Forskrift om behandling av personopplysninger (personopplysningsforskriften).

Forskrift 21. desember 2000 nr. 1385. Forskrift om pasientjournal (pasientjournalforskriften).

Forskrift 22. mai 2001 nr. 651. Forskrift om stønad til dekning av utgifter til undersøkelse og behandling hos lege og i private medisinske laboratorie- og røntgenvirksomheter. (forskrift om stønad til behandling av lege m.v.). *[Opphevet]*.

Forskrift 31. august 2001 nr. 1016. Forskrift om helse, miljø og sikkerhet i petroleumsvirksomheten (rammeforskriften) (rammeforskrift for petroleumsvirksomheten).

Forskrift 21. desember 2001 nr. 1477. Forskrift om innsamling og behandling av opplysninger i Kreftregisteret (kreftregisterforskriften).

Forskrift 20. desember 2002 nr. 1731. Forskrift om internkontroll i sosial- og helsetjenesten (internkontrollforskrift i sosial/helsetjenesten).

Forskrift 27. juni 2003 nr. 792. Forskrift om kvalitet i pleie- og omsorgstjenestene for tjenesteyting etter lov av 19. november 1982 nr. 66 om helsetjenesten i kommunene og etter lov av 13. desember 1991 nr. 81 om sosiale tjenester m.v. (forskrift om kvalitet i pleie- og omsorgstjenestene).

Forskrift 21. november 2003 nr. 1362. Forskrift om strålevern og bruk av stråling (strålevernforskriften).

Forskrift 19. desember 2003 nr. 1594. Instruks om koordinering av tilsynet med helse, miljø og sikkerhet i petroleumsvirksomheten på norsk kontinentalsokkel, og på enkelte anlegg på land (instruks om Petroleumstilsynet).

Forskrift 19. mars 2004 nr. 537. Forskrift om internkontroll for å oppfylle akvakulturlovgivningen (forskrift om IK-Akvakultur).

Forskrift 17. juni 2005 nr. 610. Forskrift om smittevern i helsetjenesten (smittevernforskriften).

Forskrift 17. juni 2005 nr. 672. Forskrift om tiltak for å forebygge og begrense konsekvensene av storulykker i virksomheter der farlige kjemikalier forekommer (storulykkeforskriften).

Forskrift 2. september 2005 nr. 1010. Forskrift om innsamling og behandling av opplysninger i Forsvarets helseregister (forskrift om forsvarets helseregister).

Forskrift 15. desember 2005 nr. 1690. Forskrift om medisinsk utstyr (forskrift om medisinsk utstyr).

Forskrift 26. april 2006 nr. 456. Forskrift om vern mot støy på arbeidsplassen (støyforskriften).

Forskrift 3. juli 2007 nr. 825. Forskrift om sikring av havner og havneterminaler mot terrorhandlinger mv (forskrift om sikring av havner mot terror).

Forskrift 7. desember 2007 nr. 1389. Forskrift om innsamling og behandling av pasientopplysninger i Norsk pasientregister (Norsk pasientregisterforskriften).

Forskrift 7. mars 2008 nr. 222. Forskrift om krav til kvalitet og sikkerhet ved håndtering av humane celler og vev (forskrift om humane celler og vev).

Forskrift 3. april 2008 nr. 320. Forskrift om legemiddelhåndtering for virksomheter og helsepersonell som yter helsehjelp (forskrift om legemiddelhåndtering).

Forskrift 22. september 2008 nr. 1080. Forskrift om risikostyring og internkontroll (forskrift om risikostyring og internkontroll).

Forskrift 8. oktober 2008 nr. 1130. Forskrift om autorisasjon, lisens og spesialistgodkjenning for helsepersonell med yrkeskvalifikasjoner fra andre EØS-land (forskrift om helsepersonell fra EØS-land).

Forskrift 15. oktober 2009 nr. 1287. Forskrift om elektronisk kommunikasjon ved fremsetting av krav om direkte økonomisk oppgjør til Helseøkonomiforvaltningen (HELFO) (forskrift om elektronisk kommunikasjon (HELFO)).

Forskrift 18. desember 2009 nr. 1639. Forskrift om behandling av helseopplysninger i Egenandelsregisteret (egenandelsregisterforskriften).

Annet særskilt regelverk

4. desember 1672. Forordning om Medicis oc Apotecker &c (Christian 5tes forordning av 1672). *[Utdatert]*.

7. juni 1979. Retningslinjer for rettighetshavers egenkontroll / Guidelines for the licensees internal control (Oljedirektoratets retningslinjer). *[Opphevet]*.

7. august 2006. Norm for informasjonssikkerhet i helsesektoren (sikkerhetsnormen).

Tekniske standarder

NS-ISO/IEC 17799:2005 «Administrasjon av informasjonssikkerhet», Standard Norge, ISO/IEC. [Denne standarden har endret navn til NS-ISO/IEC 27002, uten endring av innholdet].

ICO/CEN EN 13606 (2007): «Health informatics – Electronic health record communication», European Committee for Standardization CEN/TC 251 – Health informatics.

NS 5814:2008 «Krav til risikovurderinger». Lysaker, Standard Norge.

EU og andre land

EP/Rdir 95/46/EF. Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.

EP/Rdir 2003/10/EF. Europaparlaments- og rådsdirektiv 2003/10/EF av 6. februar 2003 om minstekrav til helse og sikkerhet med hensyn til eksponering av arbeidstakere for risikoer i forbindelse med fysiske agenser (støy) (syttende særdirektiv i henhold til artikkel 16 nr. 1 i direktiv 89/391/EØF).

EP/Rdir 2004/23/EF. Europapalamentets og rådets direktiv 2004/23/EF af 31. marts 2004 om fastsættelse af standarder for kvaliteten og sikkerheden ved donation, udtagning, testning, behandling, præservering, opbevaring og distribution af humane væv og celler.

EP/Rdir 2005/36/EF. Europaparlaments- og rådsdirektiv 2005/36/EF av 7. september 2005 om godkjenning av yrkeskvalifikasjoner.

EP/Rdir 2007/47/EF. Europa-Parlamentets og Rådets direktiv 2007/47/EF af 5. september 2007 om ændring af Rådets direktiv 90/385/EØF om indbyrdes tilnærmelse af medlemsstaternes lovgivning om aktivt, implantabelt medicinsk udstyr, 93/42/EØF om medicinsk udstyr og direktiv 98/8/EF om markedsføring af biocidholdige produkter.

Rdir 93/42/EØF. Rådsdirektiv av 14. juni 1993 om medisinsk utstyr.

Rfo 725/2004/EF. Europaparlaments- og rådsforordning (EF) nr. 725/2004 av 31. mars 2004 om forbedret sikkerhet for fartøyer og havneanlegg.

Finland: Lag om patientens ställning og rättigheter, 17. august 1992 nr. 785.

USA: 10CFR50b. Appendix B to Part 50 – Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants. (Appendix to NRC Regulations, Title 10, Code of Federal Regulations: Requirements binding on all persons and organizations who receive a license from NRC to use nuclear materials or operate nuclear facilities).

C: Forarbeider

Norges offentlige utredninger

NOU 1984:17. «Perinatal omsorg i Norge. Helsearbeid blant svangre og fødende kvinner samt nyfødte barn». [Sosialdepartementet].

NOU 1987:10. «Internkontroll i en samlet strategi for arbeidsmiljø og sikkerhet». [Kommunal- og arbeidsdepartementet].

NOU 1987:32. «Internkontroll i virksomhetenes og tilsynsorganenes arbeide med arbeidsmiljø og sikkerhet». [Kommunal- og arbeidsdepartementet].

NOU 1992:8. «Lov om pasientrettigheter». [Sosialdepartementet].

NOU 1993:22. «Pseudonyme helseregistre». [Sosialdepartementet].

NOU 1997:19. «Et bedre personvern – forslag til lov om behandling av personopplysninger». [Justis- og politidepartementet].

NOU 1999:27. ««Ytringsfrihed bør finde Sted». Forslag til ny Grunnlov § 100». [Justis- og politidepartementet].

NOU 2000:23. «Forsikringsselskapers innhenting, bruk og lagring av helseopplysninger». [Sosial- og helsedepartementet].

NOU 2004:17. «Statlig tilsyn med kommunesektoren». [Kommunalog regionaldepartementet].

NOU 2004:18. «Helhet og plan i sosial- og helsetjenestene: Samordning og samhandling i kommunale sosial- og helsetjenester». [Helse- og omsorgsdepartementet og Arbeids- og sosialdepartementet].

NOU 2005:1. «God forskning – bedre helse: lov om medisinsk og helsefaglig forskning, som involverer mennesker, humant biologisk materiale og helseopplysninger (helseforskningsloven)». [Helse- og omsorgsdepartementet].

NOU 2006:5. «Norsk helsearkiv – siste stopp for pasientjournalene: Om arkivdepot for spesialisthelsetjenesten». [Helse- og omsorgsdepartementet].

NOU 2006:14. «Gransking av Utlendingsdirektoratet». [Arbeids- og inkluderingsdepartementet].

NOU 2009:1. «Individ og integritet: Personvern i det digitale samfunnet». [Fornyings- og administrasjonsdepartementet].

Proposisjoner

Ot.prp. nr. 72 (1982-1983). «Om lov om petroleumsvirksomhet». [Olje- og energidepartementet].

Ot.prp. nr. 34 (1986-1987). «Om endringer i personregisterloven». [Justis- og politidepartementet].

Ot.prp. nr. 48 (1989-1990). «Om lov om endringer i lov 4. februar 1977 nr. 4 om arbeidervern og arbeidsmiljø, lov 21. mai 1971 nr. 47 om brannfarlige varer, lov 14. juni 1974 nr. 39 om eksplosive varer, lov 5. juni 1987 nr. 26 om brannvern, lov 13. mars 1981 nr. 6 om

forurensninger og om avfall og lov 11. juni 1976 nr. 79 om produktkontroll - internkontroll». [Kommunaldepartementet].

Ot.prp. nr. 60 (1993-1994). «Om lov om endringer i lov av 19. november 1982 nr. 66 om helsetjenesten i kommunene og i visse andre lover». [Sosial- og helsedepartementet].

Ot.prp. nr. 10 (1998-1999). «Om lov om spesialisthelsetjenesten m.m.». [Sosial- og helsedepartementet].

Ot.prp. nr. 12 (1998-1999). «Lov om pasientrettigheter (pasientrettighetsloven)». [Sosial- og helsedepartementet].

Ot.prp. nr. 13 (1998-1999). «Om lov om helsepersonell m v (helsepersonelloven)». [Sosial- og helsedepartementet].

Ot.prp. nr. 92 (1998-1999). «Om lov om behandling av personopplysninger (personopplysningsloven)». [Justis- og politidepartementet].

Ot.prp. nr. 5 (1999-2000). «Om lov om helseregistre og behandling av helseopplysninger (helseregisterloven)». [Sosial- og helsedepartementet].

Ot.prp. nr. 67 (1999-2000). «Om lov om endringer i lov 24. mai 1929 nr. 4 om tilsyn med elektriske anlegg og elektrisk utstyr (el-tilsynsloven), lov 17. juli 1953 nr. 9 om sivilforsvaret (sivilforsvarsloven), lov 21. mai 1971 nr. 47 om brannfarlige varer samt væsker og gasser under trykk (brannfarlighetsloven), lov 14. juni 1974 nr. 39 om eksplosive varer (eksplosivloven), lov 11. juni 1976 nr. 79 om kontroll med produkter og forbrukertjenester (produktkontrolloven), lov 4. februar 1977 nr. 4 om arbeidervern og arbeidsmiljø mv. (arbeidsmiljøloven), lov 13. mars 1981 nr. 6 om vern mot forurensninger og om avfall (forurensningsloven) og lov 5. juni 1987 nr. 26 om brannvern mv. (brannvernloven)». [Kommunal- og regionaldepartementet].

Ot.prp. nr. 27 (2002-2003). «Om lov om alternativ behandling av sykdommer mv.». [Helsedepartementet].

Ot.prp. nr. 72 (2004-2005). «Om lov om barnehager (barnehageloven)». [Kunnskapsdepartementet].

Ot.prp. nr. 49 (2005-2006). «Om lov om endringer i helseregisterloven (Norsk pasientregister)». [Helse- og omsorgsdepartementet].

Ot.prp. nr. 84 (2005-2006). «Om lov om endring i arbeidsmiljøloven (varsling)». [Arbeids- og inkluderingsdepartementet].

Ot.prp. nr. 25 (2007-2008). «Om lov om endringer i helsepersonelloven og helseregisterloven (krav til helsepersonells attester, erklæringer o.l., administrative reaksjoner og forbud mot urettmessig tilegnelse av helseopplysninger)». [Helse- og omsorgsdepartementet].

Ot.prp. nr. 41 (2007-2008). «Om lov om endringer i lov 16. juni 1989 nr. 69 om forsikringsavtaler m.m.». [Justis- og politidepartementet].

Ot.prp. nr. 82 (2007-2008). «Om lov om endringer i lov 28. februar 1997 nr. 19 om folketrygd (folketrygdloven) mv.». [Helse- og omsorgsdepartementet].

Ot.prp. nr. 51 (2008-2009). «Om lov om endringer i helseregisterloven og helsepersonelloven (tilgang til behandlingsrettede helseregistre på tvers av virksomhetsgrenser og etablering av behandlingsrettede helseregistre på tvers av virksomheter)». [Helse- og omsorgsdepartementet].

Prop. 23 L (2009–2010). «Endringer i helseregisterloven og helsepersonelloven (nasjonalt register over hjerte- og karlidelser, adgang til å gi dispensasjon fra taushetsplikt for kvalitetssikring, administrasjon, planlegging og styring av helsetjenesten)». [Helse- og omsorgsdepartementet].

Meldinger

Stortingsmelding nr. 65 (1977-78). «Den ukontrollerte utblåsning på Ekofiskfeltet (Bravo-plattformen) 22. april 1977». [Olje- og energidepartementet].

Stortingsmelding nr. 67 (1981-82). «Ulykken med plattformen «Alexander L. Kielland»».

Stortingsmelding nr. 17 (2002-2003). «Om statlige tilsyn (tilsynsmeldingen)». [Arbeids- og administrasjonsdepartementet].

Stortingsmelding nr. 22 (2007-2008). «Samfunnssikkerhet. Samvirke og samordning». [Justis- og politidepartementet].

Stortingsmelding nr. 47 (2008-2009). «Samhandlingsreformen. Rett behandling – på rett sted – til rett tid». [Helse- og omsorgsdepartementet].

Stortingspublikasjoner

Dokument nr. 8:44 (1993-94). (Representantforslag).

Innst.O. nr. 48 (1983-1984). «Innstilling fra sjøfarts- og fiskerikomiteen om lov om endringer i lov 9. juni 1903 nr. 7 om Statskontrol med Skibes Sjødygtighed m.v. og lov 22. mai 1902 nr. 10 Almindelig borgerlig straffelov». [Sjøfarts- og fiskerikomiteen].

Innst.O. nr. 43 (1989-1990). «Om lov om endringer i lov 4. februar 1977 nr. 4 om arbeidervern og arbeidsmiljø, lov 21. mai 1971 nr. 47 om brannfarlige varer, lov 14. juni 1974 nr. 39 om eksplosive varer, lov 5. juni 1987 nr. 26 om brannvern, lov 13. mars 1981 nr. 6 om forurensninger og om avfall og lov 11. juni 1976 nr. 79 om produktkontroll – internkontroll». [Forbruker- og administrasjonskomiteen].

Innst.O. nr. 110 (2008-2009). «Innstilling fra helse- og omsorgskomiteen om lov om endringer i helseregisterloven og helsepersonelloven (tilgang til behandlingsrettede helseregistre på tvers av virksomhetsgrenser og etablering av behandlingsrettede helseregistre på tvers av virksomheter)».

D: Avgjørelser

Høyesterett

Rt. 1977 s. 1035. *«Sykejournaldommen».*

Rt. 1984 s. 337. *«Sikkerhetsopplæring, Kiellandplattformen».*

Rt. 1995 s. 278. *«Stillasdommen».*

Rt. 2002 s. 654. *«Barnehagedommen».*

Rt. 2003 s. 1546. *«Røykedommen».*

Rt. 2006 s. 1275. *«Utlevering av pasientjournaler».*

Rt. 2007 s. 1684. *«Ammoniakkutslipp».*

Andre

Borgarting lagmannsrett: LB-2006-1155. *«Utlevering av pasientjournaler».*

Personvernnemnda: PVN-2004-01. *«STAMI».*

Preimplantasjonsdiagnostikknemnda: PGD-2008-53. *«Genetisk veiledning – farens rett til ikke å vite».*

Sivilombudsmannen: Somb-2008-18. *«Pasienters rett til å påklage pålegg til deres lege om utlevering av journalopplysninger om dem».*